

网络安全基础

NETWORK SECURITY ESSENTIALS

廉龙颖　主编
游海晖　武狄　副主编

清华大学出版社

网络安全基础

廉龙颖　主编
游海晖　武　狄　副主编

清华大学出版社
北　京

内 容 简 介

本书全面介绍了计算机网络安全的总体情况和发展趋势。全书共分为10章，系统地讲述网络安全的基础知识(网络安全概述和网络安全基础)，网络安全攻击技术(黑客与隐藏IP技术，网络扫描与网络监听，网络攻击，计算机病毒)，网络安全防御技术(身份认证与访问控制技术，防火墙技术，入侵检测技术，密码学，无线网络安全)及网络安全工程(网络安全方案设计)。

本书概念清晰，表达深入浅出，内容翔实，重点突出，实用性强，课后习题丰富，配套视频资源齐全，易于线上与线下教学相结合使用。

本书可作为信息安全、计算机、网络工程等专业本科生的教材，也可供从事相关教学、科研和工程工作的人员参考。

图书在版编目(CIP)数据

网络安全基础/廉龙颖主编. —北京：清华大学出版社，2020.3
ISBN 978-7-302-54583-5

Ⅰ. ①网…　Ⅱ. ①廉…　Ⅲ. ①计算机网络—网络安全—高等学校—教材　Ⅳ. ①TP393.08

中国版本图书馆CIP数据核字(2019)第295922号

责任编辑：刘向威
封面设计：文　静
责任校对：焦丽丽
责任印制：

出版发行：清华大学出版社
网　　址：http://www.tup.com.cn，http://www.wqbook.com
地　　址：北京清华大学学研大厦A座　　**邮　　编**：100084
社 总 机：010-62770175　　**邮　　购**：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质量反馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
课件下载：http://www.tup.com.cn，010-83470236
印 刷 者：
装 订 者：
经　　销：全国新华书店
开　　本：185mm×260mm　　**印　　张**：13.5　　**字　　数**：324千字
版　　次：2020年4月第1版　　**印　　次**：2020年4月第1次印刷
印　　数：1～1500
定　　价：39.00元

产品编号：084403-01

前　言

随着计算机网络的发展，网络的开放性、共享性随之增强，互连程度随之加深。与此同时，网络入侵事件日益增多，网络安全问题也相应日益严重。许多大学计算机相关专业都开设了“网络安全技术”课程，以培养网络安全方面的专业人才。网络安全是一门涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术等多种学科的综合性科学。网络安全在总体上可以分为网络攻击技术和网络防御技术两大方面。

本书共分为10章。第1章网络安全概述，介绍网络安全的基础知识，着重介绍研究网络安全的重要性；第2章网络基础，介绍TCP/IP、网络安全协议；第3章网络攻击技术，介绍黑客，并详细介绍黑客攻击的各种原理和技术，为读者学习防御技术打下基础；第4章计算机病毒，着重介绍计算机病毒及检测病毒的方法；第5章身份认证与访问控制技术，详细介绍身份认证、访问控制与数字签名的原理及应用；第6章防火墙技术，详细介绍防火墙原理及类型；第7章入侵检测技术，详细介绍入侵检测结构与类型；第8章密码学，着重介绍对称密码体制与非对称密码体制；第9章无线网络安全，详细介绍无线局域网安全技术；第10章网络安全方案设计，通过一个网络安全方案实例阐述网络安全方案设计方法。

本书主要特色如下。

(1) 配有基于工程教育专业认证的教学大纲。针对计算机专业的工程教育专业认证要求，本书编写了网络安全教学大纲作为本书的配置资料，为计算机专业教师提供参考。

(2) 配有丰富的课后习题。针对每一章的内容，提供了填空题、选择题、判断题、简答题等题型，并为教师提供习题解析与参考答案，便于考试和教学。

(3) 配有思维导图形式的每章小结。针对每一章的重点和难点内容进行总结，并以思维导图的形式呈现，便于学生预习和复习。

(4) 配有全部教学视频。每一章均有配套的教学视频，便于学生线上自学和复习。

本书可作为计算机、信息安全等专业本科生的教材，也可作为广大网络安全工程师、网络管理人员和计算机用户的参考书。通过学习本书，读者将掌握必要的网络安全知识，并且能够利用这些基础知识和相应的安全防护工具来保护系统。

本书第1～4、7、8章由廉龙颖编写，第5、6章由游海晖编写，第9、10章由武狄编写。本书在编写过程中参阅了大量文献，无法一一列举，在此一并向相关作者表示衷心的感谢。

网络安全学科内容广泛，发展迅速。由于编者水平有限，编写时难免有疏漏和不足，对书中存在的问题，殷切希望广大读者批评指正。

编　者

2019年10月

目　录

第1章　网络安全概述

【本章学习目标】

- 了解网络安全的定义
- 掌握网络安全的三大属性
- 了解网络安全面临的威胁
- 掌握网络安全的层次体系
- 掌握网络安全模型
- 了解网络安全评估标准
- 了解网络安全相关法律法规

网络安全是一门涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学、数论、信息论等多种学科的综合性科学。随着21世纪信息技术的快速发展和广泛应用，信息资源共享给人们的工作和生活带来了极大的便利，与此同时，网络安全问题日益突显。

1.1　网络安全概念

1.1.1　安全定义

在信息革命的演进过程中，传统互联网、移动互联网、物联网快速发展起来，成为继陆、海、空、天之后的第五大空间，被称为网络空间。在网络空间里，信息安全问题的内涵和外延也在不断扩大，最终扩大到了整个网络空间。

1. 信息安全

目前，国内外对信息安全尚无统一确切的定义。国际标准化组织(ISO)提出信息安全(Information Security)的定义是：为数据处理系统建立和采取的技术及管理保护，保护计算机硬件、软件、数据不因偶然及恶意的原因而遭到破坏、更改和泄露。

《中华人民共和国计算机信息系统安全保护条例》中将信息安全定义为：计算机信息系统的安全保护，应当保障计算机及其相关的配套设备、设施(含网络)的安全及运行环境的安全，保障信息的安全，保障计算机功能的正常发挥，以维护计算机信息系统安全运行。其主要功能为防止信息被非授权泄露、更改、破坏或使信息被非法的系统辨识与控制，确保信息的完整性、保密性、可用性。

2. 网络安全

在计算机网络产生之前，网络安全(Network Security)主要是指通信安全，重点关注的是信息加密。计算机网络产生后，网络安全中的网络主要是指计算机网络，网络安全是指保护计算机网络不因偶然及恶意因素的影响而遭到破坏、更改、泄露，保障计算机系统连续、可靠、正常地运行，保障网络服务不中断。

ITU-T X.800 标准对网络安全进行了逻辑上的定义，具体内容如下。

(1) 安全攻击(Security Attack)：指损害机构所拥有信息的安全的任何行为。

(2) 安全机制(Security Mechanism)：指设计用于检测、预防安全攻击或者恢复系统的机制。

(3) 安全服务(Security Service)：指采用一种或多种安全机制以抵御安全攻击、提高机构的数据处理系统安全和信息传输安全的服务。

随着"三网融合"的发展，网络安全领域也从计算机网络延伸到物联网和有线电视网络。近年来，网络安全进一步向物理世界和虚拟世界延伸，包括与国家基础设施密切相关的工业控制网络或系统(如电力系统、交通系统等)、虚拟的社交网络等，网络安全上升到了网络空间安全。

3. 网络空间安全

网络空间安全(Cyberspace Security)研究网络空间中的安全威胁和防护问题，即在有敌手的对抗环境中，研究信息在产生、传输、存储、处理的各个环节中所面临的威胁和防御措施以及网络和系统本身的威胁和防护机制。

信息安全、网络安全与网络空间安全之间存在异同。信息安全使用范围比较广，包括线下和线上的信息安全，既可以指传统的信息系统安全，也可以指网络安全或网络空间安全，但无法完全替代网络安全与网络空间安全的内涵；网络安全、网络空间安全的核心都是信息安全问题，只是出发点和侧重点有所不同。网络安全可以指信息安全或网络空间安全，侧重点是线上安全和网络社会安全；网络空间安全可以指信息安全或网络安全，但侧重点是与陆、海、空、天并列的空间概念。

1.1.2 网络安全属性

网络安全具有保密性、完整性和可用性三个基本属性。

1. 保密性

保密性是指保证信息与信息系统不被非授权者所获取与使用，其主要防范措施是密码技术。从技术层面上讲，任何传输线路，包括电缆(双绞线或同轴电缆)、光缆、微波和卫星，都可能被窃听。是否提供保密性安全服务取决于如下若干因素。

(1) 需保护数据的位置：数据可能存放在个人计算机或服务器、局域网的线路上，或其他流通介质如 U 盘、光盘等，也可能流经一个完全公开的媒体，如经过互联网或通信卫星。

(2) 需保护数据的类型：数据单元可以是本地文件和网络协议所携带的数据和网络协议的信息交换，如一个协议数据单元。

(3) 需保护数据的数量或部分：保护整个数据单元、部分数据单元和协议数据单元。

(4) 需保护数据的价值：被保护数据的敏感性，以及数据对用户的价值。

2. 完整性

完整性是指信息是真实可信的，其发布者不被冒充，来源不被伪造，内容不被篡改，其主要防范措施是校验与认证技术。

破坏信息的完整性既有人为因素，也有非人为因素。人为因素包括有意和无意两种，前者是非法分子对计算机进行入侵，合法用户越权对数据进行处理，以及隐藏破坏性程序，如计算机病毒、时间炸弹和逻辑陷阱等；后者是指操作失误或使用不当。非人为因素是指通信传输中的干扰噪声、系统硬件或软件的差错等。

3. 可用性

可用性是指保证信息与信息系统可被授权人正常使用，其主要范措施是确保信息与信息系统处于一个可靠的运行状态之下。

网络可用性还包括在某些不正常条件下继续运行的能力。对网络可用性的破坏，包括使合法用户不能正常访问资源和使严格要求时间的服务不能得到及时响应。影响网络可用性的因素包括人为与非人为两种。前者是指非法占用网络资源，切断或阻塞网络通信，降低网络性能，甚至使网络瘫痪等；后者是指灾害事故（火、水、雷击等）和系统死锁、系统故障等。

1.1.3 保障网络安全的三大支柱

网络安全不仅是一个纯技术问题，单凭技术因素确保网络安全是不可能的。保障网络安全无论对国家而言还是对组织而言都是一个复杂的系统工程，需要多管齐下，综合治理。目前普遍认为网络安全技术、网络安全法律法规和网络安全标准是保障网络安全的三大支柱。

1. 网络安全技术

各种网络安全技术的应用主要在技术层面上为网络安全提供具体的保障。目前主要采用的网络安全技术有网络安全扫描技术、数据加密技术、防火墙技术、入侵检测技术、病毒诊断与防治技术等。尽管网络安全技术的应用在一定程度上对网络的安全起到了很好的保护作用，但它并不是万能的，由于管理疏忽等原因而引起的网络安全事故仍然不断发生。

2. 网络安全法律法规

国家、地方以及相关部门针对网络安全的需求，制定有关网络安全的法律法规，从法律层面规范人们的行为，使网络安全工作有法可依，使相关违法犯罪行为得到处罚，促使组织和个人依法制作、发布、传播和使用网络，从而达到保障网络安全的目的。目前，我国已建立起了基本的网络安全法律法规体系，但随着网络安全形势的发展，网络安全立法的任务依然非常艰巨，许多相关法律法规还有待建立或进一步完善。

3. 网络安全标准

建立统一的网络安全标准，其目的是为网络安全产品的制造、网络安全信息系统的构建、企业或组织安全策略的制定、安全管理体系的构建以及安全工作评估等提供统一的科学依据。随着网络技术的不断发展和网络安全形势的变化，不但网络安全标准的数量在不断增加，而且许多标准的版本也在不断更新。

1.1.4 网络安全威胁

自1994年我国正式接入互联网（Internet）以来，中国互联网的规模迅速扩大，应用迅速发展。从中国互联网络信息中心（CNNIC）发布的第44次《中国互联网络发展状况统计报

告》中可获悉：截至2019年6月30日，我国网民数量达8.54亿，互联网普及率为61.2%。随着我国网络覆盖范围显著扩大、连接速度不断提升、使用费用持续降低，互联网与各产业的融合程度进一步加深。互联网的基础资源保有量稳中有升，资源应用保持增长态势。然而，目前互联网安全状况不容乐观，各种网络安全事件与2018年同期相比有明显增加。国家计算机网络应急技术处理协调中心（CNCERT）在《2018年中国互联网网络安全报告》中指出，2018年我国境内感染计算机恶意程序的主机数量约655万台，通过自主捕获和厂商交换获得的移动互联网恶意程序数量超过283万个，同比增长11.7%。了解网络面临的各种威胁，防范和消除这些威胁，实现真正的网络安全，已经成为网络发展中最重要的事情。

所谓安全威胁，是指某个人、物、事件或概念对某一资源的保密性、完整性或可用性所造成的危险。网络安全威胁主要来自于以下4个方面。

1. 网络的缺陷

因特网的共享性和开放性使网络上信息安全存在先天不足，因为其赖以生存的TCP/IP协议族缺乏相应的安全机制，所以因特网最初的设计考虑的是该网不会因局部故障而影响信息的传输，基本没有考虑安全问题，因此它在安全可靠、服务质量、带宽和方便性等方面存在着不适应性。

2. 软件的漏洞

随着软件系统规模的不断增大，系统中的安全漏洞或“后门”也不可避免地存在，比如我们常用的操作系统，无论是Windows还是UNIX几乎都存在或多或少的安全漏洞，众多服务器、浏览器、桌面软件都被发现存在各种安全隐患。

3. 黑客的攻击

对于大家来说，黑客不再是一个高深莫测的群体，黑客技术逐渐被越来越多的人掌握和发展。目前，据不完全统计，世界上有30多万个黑客网站，这些站点都会介绍一些攻击方法和攻击软件的使用以及系统漏洞，因而系统、站点遭受攻击的可能性就变大了。尤其是现在还缺乏针对网络犯罪卓有成效的反击和跟踪手段，导致黑客攻击的隐蔽性强，破坏力大，这是网络安全的主要威胁。

4. 管理的欠缺

网络系统的严格管理是企业、机构及个人用户免受攻击的重要措施。事实上，很多企业、机构及个人用户的网站或系统都疏于这方面的管理。据IT界企业团体ITAA的调查显示，美国90%的IT企业对黑客攻击防备不足。

网络安全面临的主要威胁类型及情况描述如表1-1所示。

表1-1　网络安全的主要威胁类型及描述

威胁类型	情况描述
网络窃听	网络传输信息被窃听
窃取资源	盗取系统重要的软件、硬件、信息和资料等资源
讹传信息	攻击者获得某些信息后，发送给他人
伪造信息	攻击者将伪造的信息发送给他人
篡改发送	攻击者对合法用户之间的通信信息篡改后，发送给他人
非所有权访问	通过口令、密码和系统漏洞等手段获取系统访问权
截获/修改	网络系统传输中数据被截获、删除、修改、替换或破坏

威胁类型	情况描述
拒绝服务攻击	攻击者以某种方式使系统响应减慢甚至瘫痪，使网络难以正常服务
行为否认	通信实体否认已经发生的行为
旁路控制	攻击者发掘系统的缺陷或安全脆弱性
人为疏忽	已授权用户为了利益或由于粗心将信息泄露给未授权用户
信息泄露	信息被泄露或暴露给非授权用户
物理破坏	通过计算机及其网络或部件进行破坏，或绕过物理控制非法访问
病毒木马	利用计算机病毒或木马等恶意软件进行破坏或恶意控制他人系统
服务欺骗	欺骗合法用户或系统，骗取他人信任以便谋取私利
设置陷阱	设置陷阱系统或部件，骗取特定数据以违反安全策略
资源耗尽	故意超负荷使用某一资源，导致其他用户服务中断
消息重发	重发某次截获的备份合法数据，达到信任非法侵权目的
冒名顶替	假冒他人或系统用户进行活动
媒体废弃物	利用媒体废弃物得到可利用信息，以便非法使用
网络信息战	为国家或集团利益，通过信息战进行网络破坏或恐怖袭击

1.2 网络安全体系结构

学习掌握网络安全体系结构，可以更好地理解网络安全相关的各种体系、结构、关系和构成要素等。

1.2.1 网络安全攻防体系

网络安全的研究内容主要分成两大体系：攻击和防御。网络安全攻防体系研究的内容如图 1-1 所示。

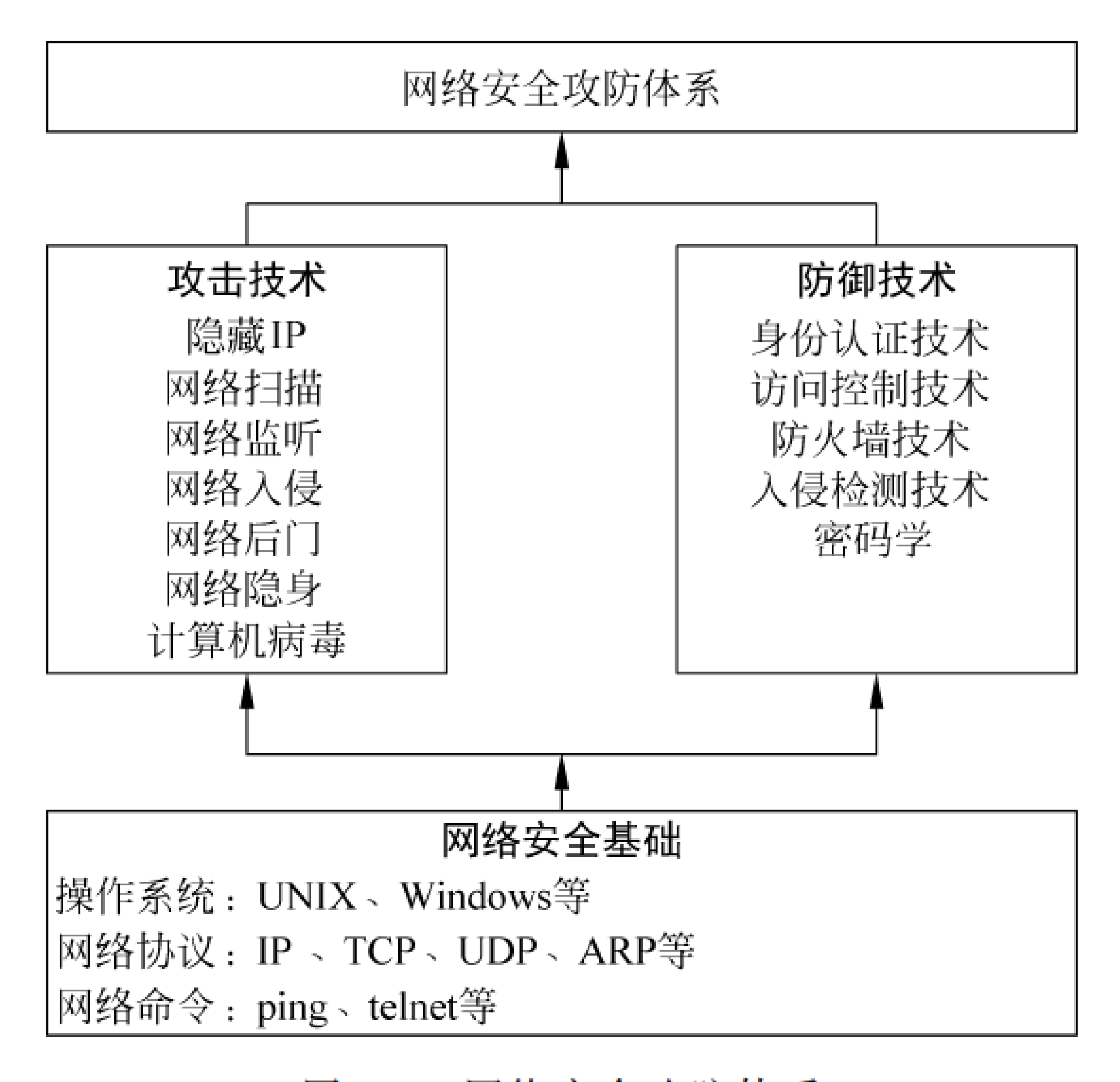


图 1-1　网络安全攻防体系

作为研究网络安全技术的基础，首先要掌握一些网络基础知识：第一，两大主流操作系统，即 UNIX 和 Windows 操作系统；第二，常用的网络安全协议，包括 IP、TCP、UDP、ARP 等；第三，常用的网络命令，如 ping、telnet 等。

1. 攻击技术

俗语称“知已知彼，百战不殆”，要想掌握网络安全防御技术，首先要掌握各种攻击技术，主要攻击技术包括隐藏 IP、网络扫描、网络监听、网络入侵、网络后门、网络隐身以及计算机病毒等。

(1) 隐藏 IP：入侵者在入侵目标计算机之前首先利用各种技术来隐藏自己的 IP 地址。

(2) 网络扫描：利用软件去扫描目标计算机的操作系统、开放的端口和漏洞，为入侵该计算机做准备。

(3) 网络监听：入侵者不主动去攻击目标计算机，而是在计算机中利用程序去监听目标计算机与其他计算机之间的通信。

(4) 网络入侵：入侵者利用各种攻击技术入侵到目标计算机中，获取信息或者破坏目标计算机。

(5) 网络后门：入侵者成功入侵到目标计算机后，会在目标计算机中种植后门程序，对目标计算机进行长期控制。

(6) 网络隐身：入侵完毕后，为了防止被管理员发现，入侵者会清除入侵痕迹。

(7) 计算机病毒：入侵者利用计算机病毒可以破坏计算机系统，影响网络运行。

2. 防御技术

防御技术主要包括身份认证与访问控制技术、防火墙技术、入侵检测技术以及密码学。

(1) 身份认证与访问控制技术：身份认证可以确保用户身份的真实性、合法性和唯一性；访问控制是针对越权使用资源的防御措施。

(2) 防火墙技术：利用防火墙，对数据包进行限制，防止被入侵。

(3) 入侵检测技术：网络一旦被入侵，利用入侵检测技术可以及时发出警报。

(4) 密码学：为了防止被监听和数据被窃取，可以利用各种适当的加密技术对敏感数据进行加密。

1.2.2 网络安全层次体系

可以从网络安全层次体系上将网络安全细分成 5 个层次的安全，包括物理层安全、网络层安全、系统层安全、应用层安全和管理层安全，如图 1-2 所示。不同安全层次反映了不同的安全问题。

图 1-2 网络安全层次体系图

1. 物理层安全

物理层安全是计算机网络信息系统运行的基础，它的安全直接影响整个网络信息的安全。物理层受到的安全威胁主要包括自然灾害、设备自然损坏和环境干扰等。物理层安全技术主要包括环境安全技术、硬件访问控制技术及防电磁泄露技术等。

(1) 环境安全技术。环境安全指网络设备所在的物理环境的湿度、温度及空气含尘浓度符合规定，同时噪声干

扰、电磁干扰、振动及静电干扰在规定范围内。

(2) 硬件访问控制技术。硬件访问控制技术是指通过硬件功能防止用户不通过访问控制系统而进入计算机系统,例如智能卡、生物特征认证等。

(3) 防电磁泄露技术。计算机在工作时会产生电磁发射,电磁发射可被高灵敏的接收设备接收并进行分析、还原,造成计算机的信息泄露。目前主要使用屏蔽技术来防止电磁泄露,屏蔽不但能防止电磁波外泄,而且还可以防止外部的电磁波对系统内设备进行干扰,并且在一定条件下还可以起到防止"电磁计算机病毒"攻击的作用。

2. 网络层安全

网络层安全主要指保证网络资源不被非授权用户使用,同时保证各种网络资源的完整性、可信赖性以及服务的可用性等。网络层面临的安全威胁主要来自于各种网络攻击,如DDoS攻击等。网络层是非常适合提供基于主机对主机的安全服务的。与网络层相应的安全协议可以用来在因特网上建立安全的IP通道和虚拟私有网。例如,利用它对IP包的加密和解密功能,可以简便地强化防火墙系统的防卫能力。

网络层安全性的主要优点是它具有透明性,即安全服务的提供不需要应用程序、其他通信层次和网络部件做任何改动。它的主要缺点是网络层一般对属于不同进程的包不加以区别,对所有发往同一地址的包,它将按照同样的加密密钥和访问控制策略来处理。这可能导致提供不了所需的功能,也会导致性能下降。

3. 系统层安全

系统层安全主要指操作系统的安全。操作系统用于管理计算机资源,控制整个系统的运行,它直接和硬件打交道,并为用户提供接口,是计算机软件的基础。操作系统的安全是整个计算机系统安全的基础。系统层面临的安全威胁主要来自于用户恶意破坏系统资源和系统的正常运行,危害计算机系统的可用性。

操作系统的安全目标主要包括:

(1) 对用户进行身份鉴别;

(2) 对用户操作进行存取控制;

(3) 监督系统运行;

(4) 保证系统自身的安全性和完整性。

为了实现操作系统的安全,需要建立相应的安全机制,包括访问控制、存储器保护、用户认证和隔离防护等。

4. 应用层安全

应用层安全主要指应用程序的安全。应用程序安全是指防止应用程序对支持其运行的计算机系统的安全进行破坏。应用层面临的安全威胁主要来自于恶意程序和应用程序本身的漏洞。为了实现应用层的安全,首先,用户不能安装恶意程序,例如病毒、后门程序、木马程序等;其次,编写应用程序的程序员应注意编程安全,养成良好的编程习惯,尽量避免产生安全漏洞。

要想区分一个具体文件在不同情况下的安全性要求,必须借助应用层的安全性。提供应用层的安全服务在处理单个文件安全性方面是最灵活的手段。如一个电子邮件系统可能

需要对其将发出信件的个别段落实施数字签名，较低层的协议提供的安全功能一般不会知道任何将发出信件的段落结构，从而不可能知道应该对哪一部分进行签名。只有应用层是唯一能够提供这种安全服务的层次。

5. 管理层安全

管理层安全主要包括安全技术和设备的管理、安全管理制度、人员组织规划等。管理的制度化极大程度地影响着整个网络的安全，严格的安全管理制度、明确的部门安全职责划分、合理的人员角色配置都可以在很大程度上降低其他层次的安全漏洞。

1.2.3 OSI 安全体系结构

OSI 安全体系结构的研究始于 1982 年 OSI 参考模型刚刚确立时，其成果标志是 ISO 发布了 ISO 7498-2 标准，作为 OSI 参考模型的新补充。1990 年，ITU 决定采用 ISO 7498-2 作为它的 X. 800 推荐标准，我国的国际 GB/T 9387. 2—1995《信息处理系统 开放系统互连基本参考模型第 2 部分：安全体系结构》等同于 ISO/IEC 7498-2。

OSI 安全体系结构不是能实现的标准，而是关于如何设计标准的标准。因此，具体产品不应称自己遵从这一标准。OSI 安全体系结构定义了许多术语和概念，还建立了一些重要的结构性准则。它们中有一部分已经过时，仍然有用的部分主要是安全攻击、安全服务和安全机制的定义。

(1) 安全攻击：任何可能会危及机构的信息安全的行为。

(2) 安全服务：用来检测、防范安全攻击并从中恢复系统的机制。

OSI 安全体系结构中定义了 5 大类安全服务，也称为安全防护措施。

① 鉴别服务。提供对通信中对等实体和数据来源的鉴别。对等实体鉴别针对实体本身的身份进行鉴别；数据来源鉴别对数据项是否来自于某个特定实体进行鉴别。

② 访问控制服务。对资源提供保护，以对抗非授权使用和操纵。

③ 数据机密性服务。保护信息不被泄漏或暴露给未授权的实体。机密性服务又分为数据机密性服务和业务流机密性服务。数据机密性服务包括：连接机密性服务，对某个连接上传输的所有数据进行加密；无连接机密性服务，对构成一个无连接数据单元的所有数据进行加密；选择字段机密性服务，仅对某个数据单元中所指定的字段进行加密。业务流机密性服务使攻击者很难通过网络的业务流来获得敏感信息。

④ 数据完整性服务。对数据提供保护，以对抗未授权的改变、删除或替代。完整性服务有三种类型：连接完整性服务，对连接上传输的所有数据进行完整性保护，确保收到的数据没有被插入、篡改、重排序或延迟；无连接完整性服务，对无连接数据单元的数据进行完整性保护；选择字段完整性服务，对数据单元中所指定的字段进行完整性保护。完整性服务还分为具有恢复功能和不具有恢复功能两种类型。仅能检测和报告信息的完整性是否被破坏，而不采取进一步措施的服务为不具有恢复功能的完整性服务；能检测到信息的完整性是否被破坏，并能将信息正确恢复的服务为具有恢复功能的完整性服务。

⑤ 抗抵赖性服务。指防止参与通信的任何一方事后否认本次通信或通信内容。抗抵赖性服务分为两种不同的形式：数据原发证明的抗抵赖，使发送者不承认曾经发送过这些数据或否认其内容的企图不能得逞；交付证明的抗抵赖，使接收者不承认曾收到这些数据

或否认其内容的企图不能得逞。

表 1-2 给出了网络各层提供的安全服务。

表 1-2　网络各层提供的安全服务

安全服务		网络层次						
		物理层	数据链路层	网络层	传输层	会话层	表示层	应用层
鉴别	对等实体鉴别			√	√			√
	数据来源鉴别			√	√			√
访问控制				√	√			√
数据机密性	连接机密性	√	√	√	√		√	√
	无连接机密性		√	√	√		√	√
	选择字段机密性							√
	业务流机密性						√	√
数据完整性	可恢复的连接完整性	√		√				√
	不可恢复的连接完整性				√			√
	选择字段的连接完整性			√	√			√
	无连接完整性							√
	选择字段的无连接完整性			√	√			√
抗抵赖性	数据原发证明的抗抵赖							√
	交付证明的抗抵赖							√

(3) 安全机制：用来增强组织的数据处理系统安全性和信息传递安全性的服务。

OSI 安全体系结构没有详细说明安全服务应该如何来实现。作为指南，它给出了一系列可用来实现这些安全服务的安全机制，如表 1-3 所示。其基本的机制有加密机制、数字签名机制、访问控制机制、数据完整性机制、鉴别交换机制、业务流填充机制、路由控制机制和公证机制。

表 1-3　安全服务与安全机制的关系

安全服务		安全机制							
		加密	数字签名	访问控制	数据完整性	鉴别交换	业务流填充	路由控制	公证
鉴别	对等实体鉴别	√	√			√			
	数据来源鉴别	√	√						
访问控制				√					
数据机密性	连接机密性	√						√	
	无连接机密性	√						√	
	选择字段机密性	√							
	业务机密性	√					√	√	

续表

安全服务		安全机制							
		加密	数字签名	访问控制	数据完整性	鉴别交换	业务流填充	路由控制	公证
数据完整性	可恢复的连接完整性	√			√				
	不可恢复的连接完整性	√			√				
	选择字段的连接完整性	√			√				
	无连接完整性	√	√		√				
	选择字段的无连接完整性	√	√		√				
抗抵赖性	数据原发证明的抗抵赖		√		√				√
	交付证明的抗抵赖		√		√				√

计算机网络安全体系结构三维图如图 1-3 所示。

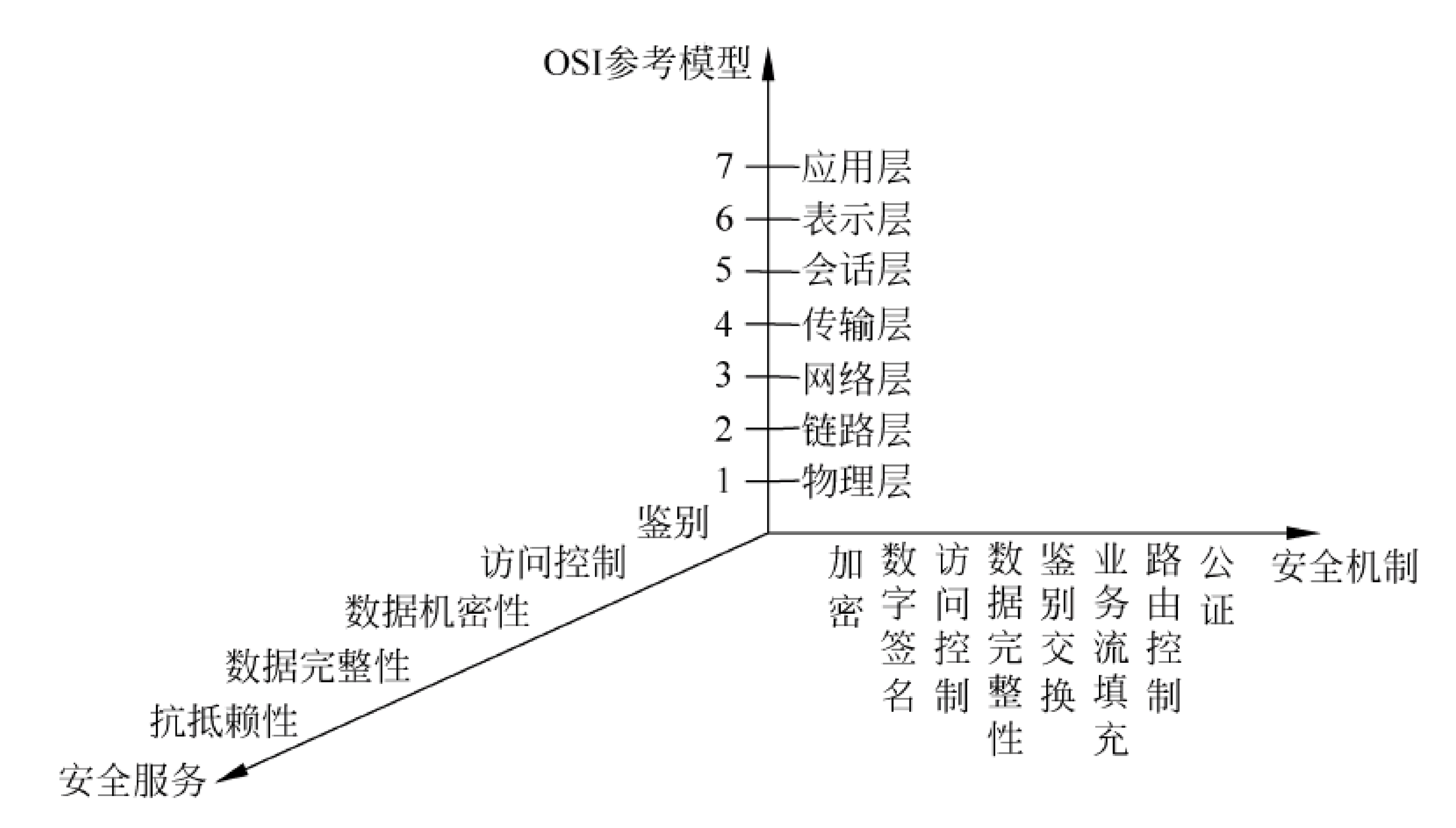


图 1-3　计算机网络安全体系结构三维图

1.3　网络安全评价

1.3.1　网络安全标准组织

国际上信息安全标准化工作兴起于 20 世纪 70 年代中期，80 年代有了较快的发展，90 年代引起了世界各国的普遍关注。目前，国际上与信息安全标准化有关的组织主要有国际标准化组织（ISO）、国际电工委员会（IEC）、美国国家标准和技术研究所（NIST）、国际电信联盟（ITU）和互联网工程任务组（IETF）。国内的安全标准组织主要有信息技术安全标准化技术委员会（CITS）及中国通信标准化协会（CCSA）下的网络与信息安全技术工作委员会。

1. 国际标准化组织

国际标准化组织始建于 1946 年，是世界上最大的非政府性标准化专门机构，它在国际标准化中占有主导地位。ISO 的主要活动是制定国际标准，协调世界范围内的标准化工作，

组织各成员国和技术委员会进行交流，以及与其他国际性组织进行合作，共同研究有关标准问题。随着人们对安全的重视不断加强，世界各地的许多企业、政府机构和其他组织把获得ISO 17799认证作为目标。ISO 17799提供了一个方便的框架以便安全策略制定者能够依据国际标准构建自己的策略。

2. 国际电工委员会

IEC是世界上成立最早的非政府性国际电工标准化机构，是联合国经社理事会(ECOSOC)的甲级咨询组织。IEC在信息安全标准化方面除了与ISO联合成立了JTC1分委员会外，还在电信、电子系统、信息技术和电磁兼容等方面成立了技术委员会，并且制定了相关国际标准，如信息技术设备安全IEC 60950等。

3. 美国国家标准和技术研究所

NIST成立于1901年，原名为美国国家标准局(NDS)，1988年8月，经美国总统批准更名为美国国家标准和技术研究所。NIST已经发行了大量的美国联邦信息处理标准出版物和特别公告，这些公告对安全管理者、设计者和实施者非常有用。其中，FIPS PUB 200(美国联邦信息与信息系统最低安全需求)规定了17个与安全相关领域的最低安全需求。

4. 国际电信联盟

国际电信联盟于1865年5月在巴黎成立，1947年成为联合国的专门机构。ITU是世界各国政府的电信主管部门之间协调电信事务的一个国际组织，它研究制定有关电信业务的规章制度，通过决议提出推荐标准，收集有关情报。其中，国际电信联盟电信标准化部门(ITU-T)已经发布了X.800系列的推荐标准，其内容覆盖了数据网络的安全，它对安全威胁、安全服务和安全机制做了详细的概述。

5. 互联网工程任务组

IETF成立于1985年，其主要任务是负责互联网相关技术规范的研发和制定。目前，IETF已成为全球互联网界最具权威的大型技术研究组织。IETF分成8个工作组，分别负责因特网路由、传输、应用等8个领域，其著名的IKE和IPSec都在RFC系列之中，还有电子邮件、网络认证和密码及其他安全协议标准。

6. 信息技术安全标准化技术委员会

CITS成立于1984年，在国家标准化管理委员会和信息产业部的共同领导下，负责全国信息技术领域及与ISO/IEC JTC1相对应的标准化工作，目前下设24个分技术委员会和特别工作组，是国内最大的标准化技术委员会，也是具有广泛代表性、权威性的信息安全标准化组织。CITS主要负责信息安全的通用框架、方法、技术和机制的标准化及国内外对应的标准化工作，其中技术安全包括开放式安全体系结构、各种安全信息交换的语义规则、有关的应用程序接口和协议引用安全功能的接口等。

7. 中国通信标准化协会

CCSA成立于2002年，是国内企事业单位经业务主管部门批准，自愿联合组织起来的开展通信技术领域标准化活动的组织。CCSA下设有线网络信息安全、无线网络信息安全、安全管理和安全基础设施4个工作组，负责研究的内容有：有线网络中电话网、互联网、传

输网、接入网等在内所有电信网络相关的安全标准；无线网络中接入、核心网、业务等相关的安全标准及安全管理工作；安全基础设施工作组中网络管理安全及与安全基础设施相关的标准。

1.3.2 P2DR2 动态安全模型

如图 1-4 所示，P2DR2 动态安全模型由策略（Policy）、防护（Protection）、检测（Detection）、响应（Response）和恢复（Restore）五要素构成，是一种基于闭环控制，主动防御，具有时间及策略特征的动态安全模型，能够构造多层次、全方位和立体的区域网络安全环境。

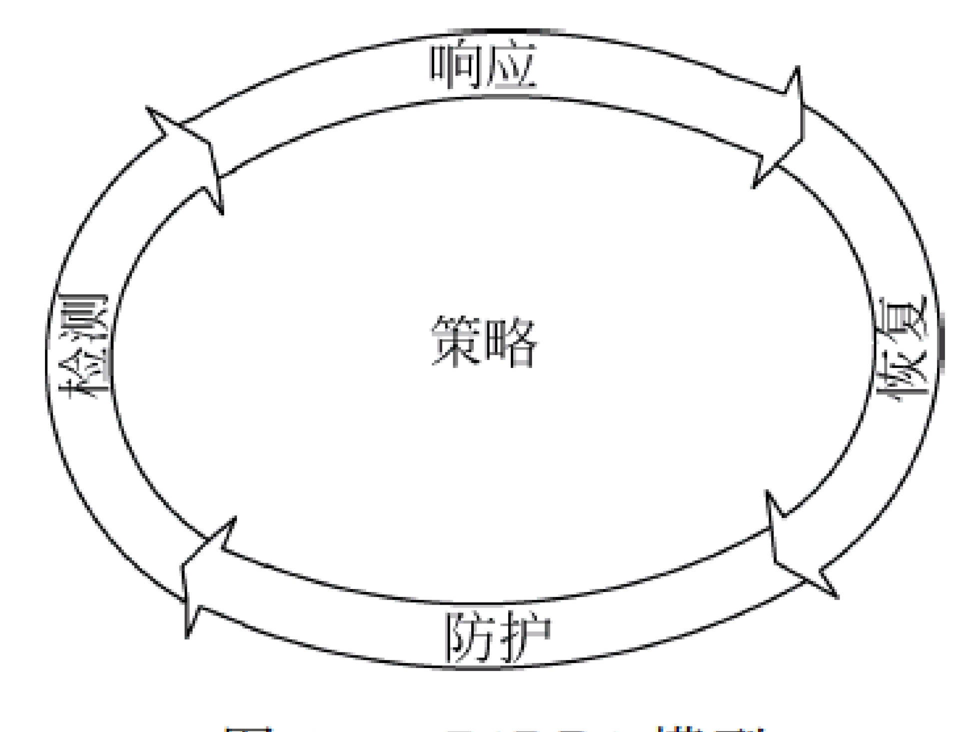


图 1-4　P2DR2 模型

（1）策略是 P2DR2 模型的核心，是规定网络要达到安全的目标而采取的各种方法和措施，所有的防护、检测、响应、恢复都是依据安全策略实施的。策略描述网络中哪些资源要得到保护，以及如何实现对它们的保护等。策略一般包括总体安全策略和具体安全策略两个部分。

（2）防护指通过修复系统漏洞、正确设计开发和安装系统来预防安全事件的发生；通过定期检查来发现可能存在的系统脆弱性；通过教育手段使用户正确使用系统，防止意外威胁；通过访问控制、监视等手段来防止恶意威胁。如用于提供边界保护和构建安全域的防火墙技术、操作系统的身份认证技术、信息传输过程中的加密技术等。

（3）检测是动态响应和加强防护的依据，通过不断地检测和监控网络，来发现新的威胁和弱点，通过循环反馈来及时做出有效的响应。检测主要包括漏洞扫描技术、IDS、IPS 等。当攻击者穿透防护时，检测功能开始发挥作用，与防护形成互补。

（4）网络一旦检测到入侵，响应就开始工作，进行入侵事件处理，阻止入侵进一步发展。如提示用户有程序要修改操作系统注册表，要求用户确认是否允许修改。响应机制要对入侵行为做出反应，记录入侵行为并通知系统管理员，采取相应的措施阻止该入侵行为。响应技术主要包括报警、反击等。

（5）恢复是指将系统还原到可用状态或原始状态，包括系统恢复和信息恢复。

1.3.3 网络安全评估标准

为实现对网络安全的定性评价，美国国防部所属的国家计算机安全中心（NCSC）在 20 世纪 90 年代提供了网络安全性标准（DoD5200.28-STD），即可信任计算机标准评估准则（Trusted Computer Standards Evaluation Criteria，TCSEC），也叫橘黄皮书（Orange Book）。该标准认为要使系统免受攻击，对应不同的安全级别，硬件、软件和存储的信息应实施不同的安全保护。安全级别对不同类型的物理安全、用户身份验证、操作系统软件的可信任性和用户应用程序分别进行了安全描述。

目前，TCSEC 已经成为现行的网络安全标准。TCSEC 将网络安全性等级划分为 A、B、C、D 等 4 类共 7 级，其中，A 类安全等级最高，D 类安全等级最低。

1. D1 级

D1 级也称为酌情安全保护，是可用的最低安全形式。该标准说明整个系统都是不可信任的。对硬件来说，没有任何保护，操作系统容易受到损害，对于用户和对存储在计算机上信息的访问权限没有身份认证。

2. C1 级

C 级有两个安全子级别：C1 和 C2，也称为自选安全保护系统，它描述了一个在 UNIX 系统上可用的级别。对硬件来说，尽管它可能受到损害，但因为存在某种程度的保护，它不再轻易受到损害。用户必须通过用户注册名和口令系统识别自己，用这种方式来确定每个用户对程序和信息拥有什么样的访问权限。

3. C2 级

除 C1 级包含的特征外，C2 级还包括其他创建受控访问环境的安全特性，该环境具有进一步限制用户执行某些命令或访问某些文件的能力。这不仅基于许可权限，而且基于身份验证级别。另外，这种安全级别要求对系统加以审核，审核可用来跟踪记录所有与安全有关的事件，比如哪些是由系统管理员执行的活动。

4. B1 级

B 级也称为被标签的安全性保护，分为三个子级别。B1 级也称为标准安全保护，是支持多级安全的第一个级别，这一级说明，一个处于强制性访问控制之下的对象不允许文件的拥有者改变其许可权限。

5. B2 级

B2 级也称为结构保护，要求计算机系统中所有对象都加标签，而且给设备分配单个或多个安全级别。这是提出的较高安全级别的对象与另一个较低安全级别的对象相互通信的第一个级别。

6. B3 级

B3 级也称为安全域级别，使用安装硬件的办法来加强域，例如，内存管理硬件用来保护安全域免遭无授权访问或其他安全域对象的修改。该级别也要求用户终端通过一条可信任途径连接到系统上。

7. A 级

A 级也称为验证设计，是当前橘黄皮书中的最高级别，包含了一个严格的设计、控制和验证过程。与前面提到的各级别一样，这一级包含了较低级别的所有特性，其设计必须是从数学上经过验证的，而且必须进行对秘密通道和可信任分布的分析。

橘黄皮书安全系统分类总结如表 1-4 所示。

表 1-4 橘黄皮书安全系统分类

评估标准	D	C1	C2	B1	B2	B3	A
安全策略							
直接访问控制			√	√			√
目标重用					√	√	

续表

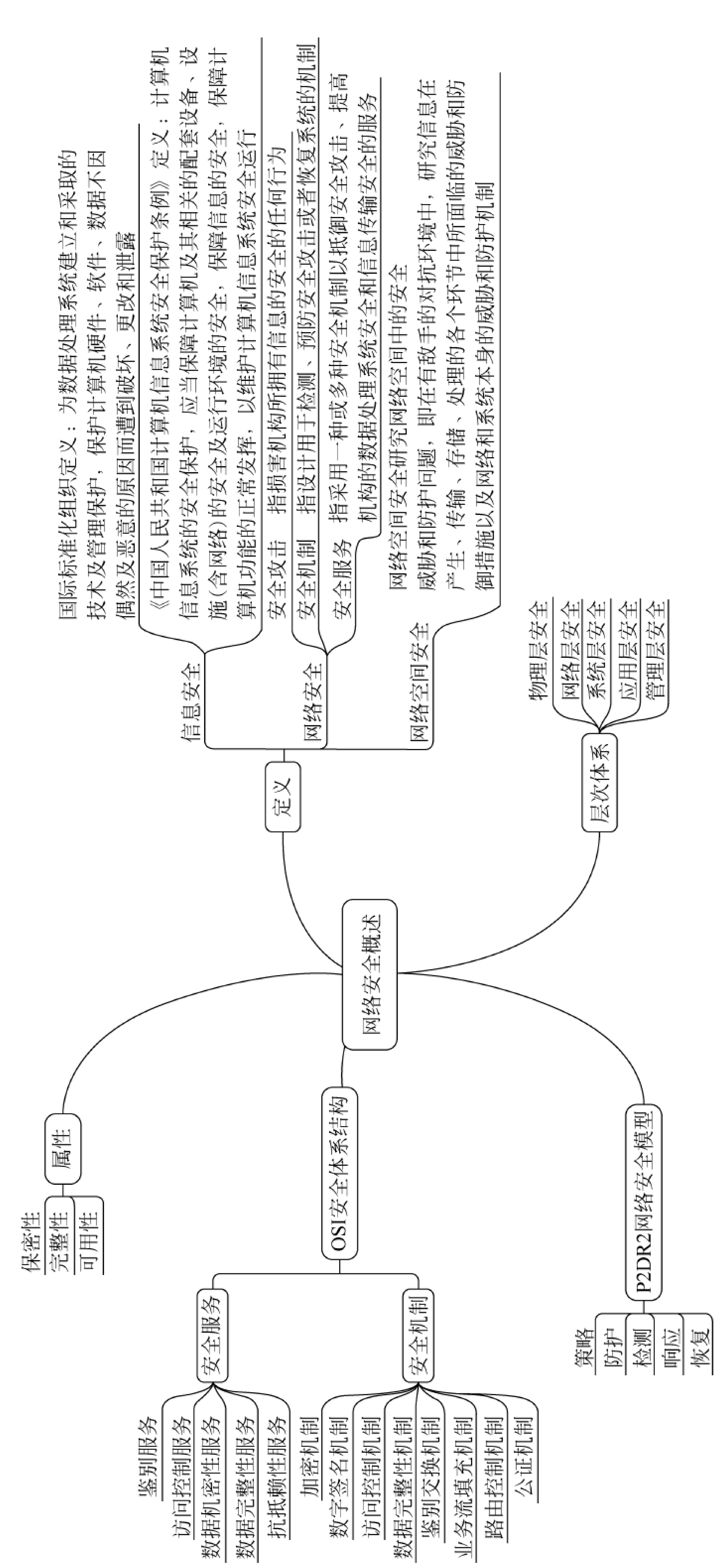
评 估 标 准	D	C1	C2	B1	B2	B3	A
标签						√	√
标签完整性					√		
被标识信息输出				√			
多层设备输出				√			
单层设备输出				√			
标记人可读输出				√			
强制访问控制				√	√		
目标敏感标签				√	√		
设备标签					√		
可说明性							
确认授权		√	√	√			
审计						√	√
可信路径					√	√	
保险							
系统体系				√	√	√	√
系统完整性				√			
安全测试				√	√	√	√
设计说明和确认				√	√	√	√
隐秘通道分析					√	√	√
可信装置管理					√	√	
配置管理					√		√
可信恢复						√	
可信分发							√
文献							
安全特性用户指南		√					
可信装置手册			√	√	√	√	√
测试文档				√			
设计文献			√		√	√	√

注：“√”表示本级有些新的或比对低一级更强的需求

1.4　网络安全法律法规

《中华人民共和国网络安全法》是为保障网络安全，维护网络空间主权和国家安全、社会公共利益，保护公民、法人和其他组织的合法权益，促进经济社会信息化健康发展而制定的，由全国人民代表大会常务委员会于 2016 年 11 月 7 日发布，自 2017 年 6 月 1 日起施行。

1.5 本章小结



网络安全概述
定义
信息安全
国际标准化组织定义：为数据处理系统建立和采取的技术及管理保护，保护计算机硬件、软件、数据不因偶然及恶意的原因而遭到破坏、更改和泄露
《中国人民共和国计算机信息系统安全保护条例》定义：计算机信息系统的安全保护，应当保障计算机及其相关的配套设备、设施(含网络)的安全及运行环境的安全，保障信息的安全，保障计算机功能的正常发挥，以维护计算机信息系统安全运行
网络安全
安全攻击 指损害机构所拥有信息的安全的任何行为
安全机制 指设计用于检测、预防安全攻击或者恢复系统的机制
安全服务 指采用一种或多种安全机制以抵御安全攻击、提高机构的数据处理系统安全和信息传输安全的服务
网络空间安全
网络空间安全研究网络空间中的安全
威胁和防护问题，即在有敌手的对抗环境中，研究信息在产生、传输、存储、处理的各个环节中所面临的威胁和防御措施以及网络和系统本身的威胁和防护机制
层次体系
物理层安全
网络层安全
系统层安全
应用层安全
管理层安全
属性
保密性
完整性
可用性
OSI安全体系结构
安全服务
鉴别服务
访问控制服务
数据机密性服务
数据完整性服务
抗抵赖性服务
安全机制
加密机制
数字签名机制
访问控制机制
数据完整性机制
鉴别交换机制
业务流填充机制
路由控制机制
公证机制
P2DR2网络安全模型
策略
防护
检测
响应
恢复

1.6 习　　题

一、填空题

1. 网络安全的三个基本属性包括保密性、完整性和(　　)。

2. P2DR2 模型中的 D 代表的含义是(　　)。

3. 目前普遍认为网络安全技术、网络安全法律法规和(　　)是保障网络安全的三大支柱。

4. (　　)层安全主要指保证网络资源不被非授权使用,同时保证各种网络资料的完整性、可依赖性以及服务的可用性等。

二、选择题

1. 计算机网络安全体系结构是指(　　)。

A. 网络安全基本问题应对措施的集合　　B. 各种网络的协议的集合

C. 网络层次结构和各层协议的集合　　D. 网络的各层次结构的总称

2. TCSEC 将计算机系统安全划分为(　　)。

A. 3 个等级 7 个级别　　B. 4 个等级 7 个级别

C. 5 个等级 7 个级别　　D. 6 个等级 7 个级别

3. 在短时间内向网络中的某台服务器发送大量无效连接请求,导致合法用户暂时无法访问服务器的攻击行为是破坏了(　　)。

A. 保密性　　B. 完整性　　C. 可用性　　D. 可控性

4. 如果访问者有意避开系统的访问控制机制,则访问者对网络设备及资源进行非正常使用属于(　　)。

A. 破坏数据完整性　　B. 非授权访问

C. 信息泄露　　D. 拒绝服务攻击

5. 未授权的实体得到了数据的访问权,这样做破坏了安全特性中的(　　)。

A. 保密性　　B. 完整性　　C. 可用性　　D. 可控性

6. 篡改信息的攻击行为是破坏了网络安全中的(　　)。

A. 保密性　　B. 完整性　　C. 可用性　　D. 可控性

7. 以下(　　)不是信息安全目标。

A. 保密性　　B. 完整性　　C. 可用性　　D. 及时性

8. 在 P2DR2 模型中,作为整个计算机网络系统安全行为准则的是(　　)。

A. 策略　　B. 防护　　C. 检测　　D. 响应

9. 完整性是指信息是真实可信的,其发布者不被冒充,来源不被伪造,内容不被篡改,主要防范措施是(　　)。

A. 密码技术　　B. 校验与认证技术

C. 可靠运行　　D. 防止非法占用网络资源

10. 以下(　　)不属于物理层安全技术。

A. 环境安全技术　　B. 硬件访问控制技术

C. 病毒检测技术　　D. 防电磁泄露技术

三、判断题

1. 保密性是指保证信息与信息系统不被非授权者所获取与使用，主要防范措施是密码技术。

2. 网络安全威胁主要来源于网络的缺陷、软件的漏洞、黑客的攻击以及管理的欠缺。

3. 系统层安全威胁主要包括自然灾害、设备自然损坏和环境干扰等。

4. 应用层面临的安全威胁主要来自于恶意程序和应用程序本身的漏洞。

5. TCSEC 将网络安全性等级划分 为 A、B、C、D 等 4 类共 7 级，其中，A 类安全等级最低，D 类安全等级最高。

四、简答题

1. P2DR2 模型的五要素是什么？

2. 在 OSI 安全系统结构中定义的 5 类安全服务是什么？

3. 在 OSI 安全系统结构中定义的 8 类特定的安全机制是什么？

4. ISO 提出的信息安全定义是什么？

第 2 章　网 络 基 础

【本章学习目标】

- 了解 OSI 参考模型和 TCP/IP 体系结构各层的主要功能
- 熟悉 IP、ICMP、ARP、TCP 和 UDP
- 理解 TCP/IP 层次安全性
- 掌握 IPSec 协议工作原理

2.1　OSI 参考模型

OSI(Open System Interconnection)参考模型是由 ISO 制定的标准化开放式系统互连参考模型，是一个逻辑上的定义，也是一个规范，它把网络从逻辑上分为 7 层，每一层都有相关和相对应的物理设备。它的最大优点是将服务、接口和协议这三个概念明确地区分开来，通过 7 个层次化的结构模型使不同系统、不同网络之间实现可靠的通信。图 2-1 是 OSI 参考模型的 7 层结构。

应用层
表示层
会话层
传输层
网络层
数据链路层
物理层

第7层（上）……第1层（下）

图 2-1　OSI 参考模型

1. 物理层

物理层是 OSI 参考模型的最低层或第 1 层。物理层的协议产生并检测电压以便发送和接收携带数据的信号，就是在通信信道上传输原始的数据位，即相当于“信息实际如何传送”。

2. 数据链路层

数据链路层是 OSI 参考模型的第 2 层，它控制网络层与物理层之间的通信。它的主要功能是如何在不可靠的物理线路上进行数据的可靠传递，就是在物理链路上无差错地传送数据帧，即相当于“每一步该怎么走”。

3. 网络层

网络层是 OSI 参考模型的第 3 层，它的主要功能是将网络地址翻译成对应的物理地址，并决定如何将数据从发送方路由到接收方，网络层就是完成分组传送、路由选择和网络管理等工作，即相当于“数据如何到达对方”。

4. 传输层

传输层是 OSI 参考模型的第 4 层，也是最重要的一层。传输协议同时进行流量控制或是基于接收方可接收数据的快慢程度规定适当的发送速率，除此之外，传输层按照网络能处

理的最大尺寸将较长的数据包进行强制分割。传输层的主要工作就是从端到端经网络透明地传送报文,即相当于"对方在何处"。

5. 会话层

会话层是 OSI 参考模型的第 5 层,负责在网络中的两节点之间建立、维持和终止通信。会话层的功能包括:建立通信连接,保持会话过程通信连接的畅通,同步两个节点之间的对话,决定通信是否被中断以及在通信中断时决定从何处重新发送。简单地说,会话层就是完成会话的管理与数据传输的同步工作,即相当于"如何检查"。

6. 表示层

表示层是 OSI 参考模型的第 6 层,它是应用程序和网络之间的翻译官,在表示层,数据将按照网络能理解的方案进行格式化,这种格式化也因所使用网络类型的不同而不同。表示层的主要工作就是关心传递数据的语法与语义,即相当于"像什么"。

7. 应用层

应用层是 OSI 参考模型的第 7 层,负责对软件提供接口以使程序能使用网络服务,就是包含直接针对用户需要的协议,即相当于"做什么"。

OSI 参考模型作为一个开放网络通信协议族的工业标准,很容易实现不同网络技术的互联和互操作。但是,由于实现所有的 7 层模型过于复杂,效率也低,因此很少有产品完全符合 OSI 参考模型。

2.2 TCP/IP 协议族

TCP/IP 是用于计算机通信的一组协议,通常称它为 TCP/IP 协议族。采用 TCP/IP 协议族通过互联网传送信息可减少网络中的传输阻塞,方便大批量的数据在网络上传输,从而提高网络的传输效率。TCP/IP 协议族中包括上百个互为关联的协议,例如,ICMP、ARP/RARP、UDP、FTP、HTTP、SMTP 等。

1. TCP/IP 的层次结构

从协议分层模型方面来划分,TCP/IP 由 4 个层次组成,分别是网络接口层、网络层、传输层和应用层。

1) 网络接口层

网络接口层把数据链路层和物理层放在一起,对应 TCP/IP 概念模型的网络接口。对应的网络协议主要是 PPP(Point-to-Point Protocol,点对点协议)、HDLC(High Level Data Link Control,高级链路控制协议)等。

2) 网络层

网络层对应 OSI 参考模型的网络层。重要的网络层协议包括 IP(Internet Protocol,网际协议)、ICMP(Internet Control Message Protocol,网际控制报文协议)、ARP(Address Resolution Protocol,地址解析协议)和 RARP(Reverse Address Resolution Protocol,反向地址解析协议)等。

3) 传输层

传输层对应 OSI 参考模型的传输层。传输层包括 TCP(Transmission Control Protocol,传输控制协议)和 UDP(User Datagram Protocol,用户数据报协议),它们是传输

层中最主要的协议。

4）应用层

应用层对应OSI参考模型的应用层、表示层和会话层。应用层位于协议栈的顶端，它的主要任务是应用。常见的应用层协议有FTP（File Transfer Protocol，文件传输协议）、HTTP（Hyper Text Transfer Protocol，超文本传输协议）、DNS（Domain Name Service，域名服务器）和SMTP（Simple Mail Transfer Protocol，简单邮件传输协议）等。

2. OSI参考模型和TCP/IP模型比较

表2-1是OSI参考模型和TCP/IP模型的比较，同时将各种网络协议归类。

表2-1　OSI参考模型和TCP/IP模型比较

OSI参考模型	TCP/IP模型	网 络 协 议
应用层	应用层	FTP/HTTP/DNS/SMTP等
表示层		
会话层		
传输层	传输层	TCP/UDP
网络层	网络层	IP/ICMP/ARP/RARP等
数据链路层	网络接口层	PPP/HDLC等
物理层		

OSI参考模型和TCP/IP模型两种分层的主要不同之处是：TCP/IP在实现上力求简单高效，如IP层并没有实现可靠的连接，而是把它交给了传输层的TCP去实现，这样保证了IP层实现的简单性。事实上有些服务并不需要可靠的面向连接服务，如果在IP层加上可靠性控制，只能说是一种处理能力的浪费。OSI参考模型在各层的实现上有所重复，而且会话层和表示层不是对所有服务都有用，无疑这种模型有些烦琐。

3. TCP/IP工作原理

下面以使用TCP传送文件为例说明TCP/IP的工作原理。

（1）在源主机上应用层将一串字节流传送给传输层。

（2）传输层将应用层的数据流截成分组，并加上TCP报头形成TCP段，送交网络层。

（3）在网络层给TCP段加上包括源、目的主机IP地址的IP报头，生成一个IP数据报，并将IP数据报送交数据链路层。

（4）链路层在其帧的数据部分装上IP数据报，再加上源、目的主机的MAC地址和帧头，并根据其目的主机的MAC地址，将帧发往目的主机或IP路由器。

（5）在目的主机，数据链路层将帧的帧头去掉，并将IP数据报送交网络层。

（6）网络层检查IP报头，如果报头中校验和与计算结果不一致，则丢弃该IP数据报；若校验和与计算结果一致，则去掉IP报头，将TCP段送交传输层。

（7）传输层检查顺序号，判断是否是正确的TCP分组，然后检查TCP报头数据。若正确，则向源主机发确认信息；若不正确或丢包，则向源主机要求重发信息。

（8）在目的主机，传输层去掉TCP报头，将排好顺序的分组组成应用数据流送给应用程序。

这样目的主机接收到的来自源主机的字节流，就像是直接接收来自源主机的字节流一样。

2.2.1 网际协议

IP 又称网际协议，是支持网间互联的数据报协议，它与 TCP 一起构成 TCP/IP 协议族的核心，IP 层接收由更低层发来的数据包，并把该数据包发送到更高层的 TCP 或 UDP 层；相反，IP 层也把从 TCP 或 UDP 层接收来的数据包传送到更低层。IP 数据报是不可靠的，因为 IP 并没有做任何事情来确认数据包是按顺序发送的或者没有被破坏。IP 数据报中含有发送它的主机的地址（源地址）和接收它的主机的地址（目的地址）。

1. 数据报的格式

IP 数据报的格式能够说明 IP 都具有什么功能。图 2-2 是 IP 数据报的完整格式。

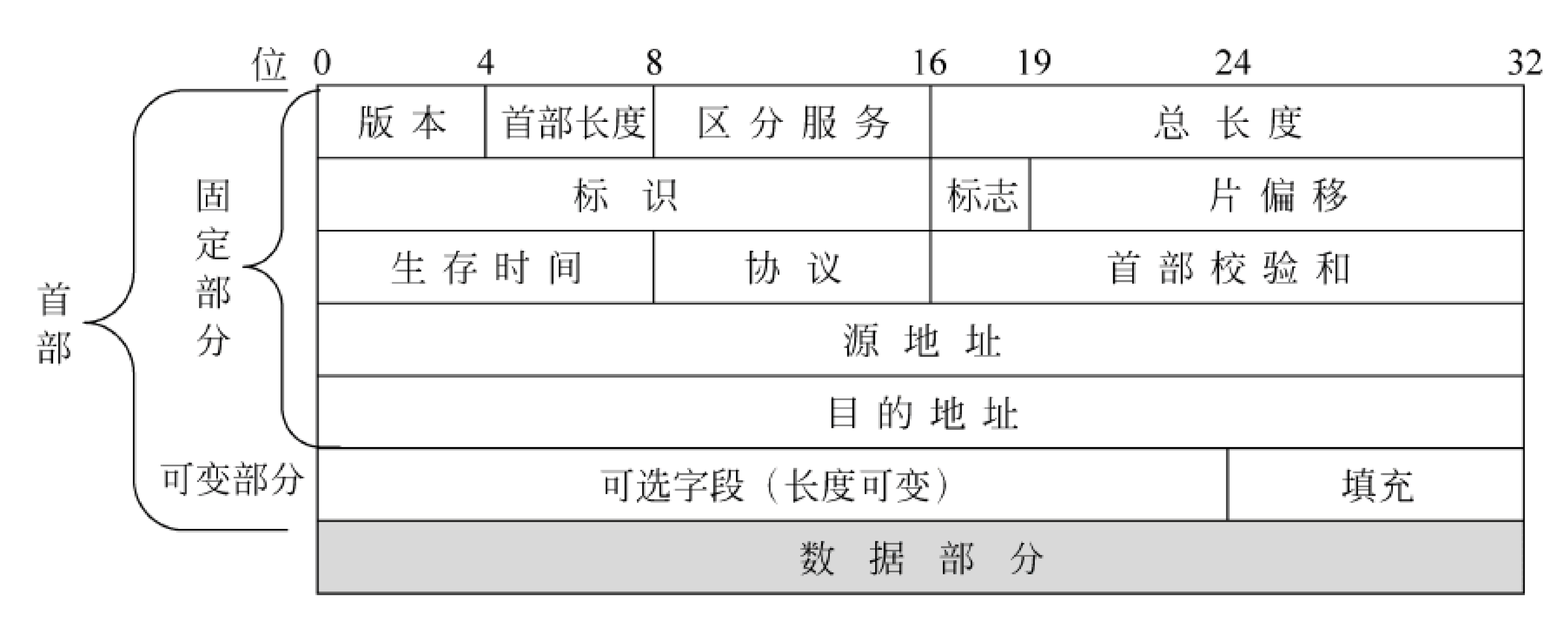


图 2-2　IP 数据报的完整格式

从图 2-2 中可看出，一个 IP 数据报由首部和数据两部分组成。首部的前一部分是固定长度，共 20 字节，是所有 IP 数据报必须具有的。在首部的固定部分的后面是一些可选字段，其长度是可变的。下面介绍首部各字段的意义。

（1）版本：占 4 位，指出当前使用的 IP 版本。

（2）首部长度：占 4 位，指出数据报协议头长度，可表示的最大十进制数值是 15。

（3）区分服务：占 8 位，用来获得更好的服务。

（4）总长度：指首部和数据之和的长度，单位为字节。总长度字段为 16 位，因此数据报的最大长度为 $2^{16}-1=65\,535$ 字节。

（5）标识：占 16 位，包含一个整数，用于识别当前数据报。

（6）标志：占 3 位，但目前只有两位有意义。标志字段中的最低位为 MF(More Fragment)，MF＝1 表示后面“还有分片”的数据报。MF＝0 表示这已是若干数据报片中的最后一个。标志字段中间的一位记为 DF(Don’t Fragment)，意思是“不能分片”，只有当 DF＝0 时才允许分片。

（7）片偏移：占 13 位，指出与源数据报的起始端相关的分片数据位置，支持目标 IP 适当重建源数据报。

（8）生存时间：占 8 位，表明数据报在网络中的寿命。

（9）协议：占 8 位，指出在 IP 处理过程完成之后，由哪种上层协议接收数据包。

（10）首部校验和：占 16 位，这个字段只检验数据的首部，但不包括数据部分。

（11）源地址：占 32 位。

（12）目的地址：占 32 位。

(13) 选项：允许 IP 支持各种选项，如安全性。

2. IPv4 的 IP 地址分类

在因特网上，为了实现连接到互联网上的节点之间的通信，必须为每个连接到互联网的节点分配一个地址，并且应当保证这个地址是全球唯一的，这就是 IP 地址。IP 地址长度为 32 位，最初设计互联网络时，为了便于寻址以及层次化构造网络，每个 IP 地址包括两个标识码(ID)，即网络 ID 和主机 ID。同一个物理网络上的所有主机都使用同一个网络 ID，网络上的一个主机(包括网络上的工作站、服务器和路由器等)有一个主机 ID 与其对应。因特网委员会定义了 5 种 IP 地址类型以适合不同容量的网络，即 A 类～E 类。5 类不同的 IP 地址格式如图 2-3 所示。

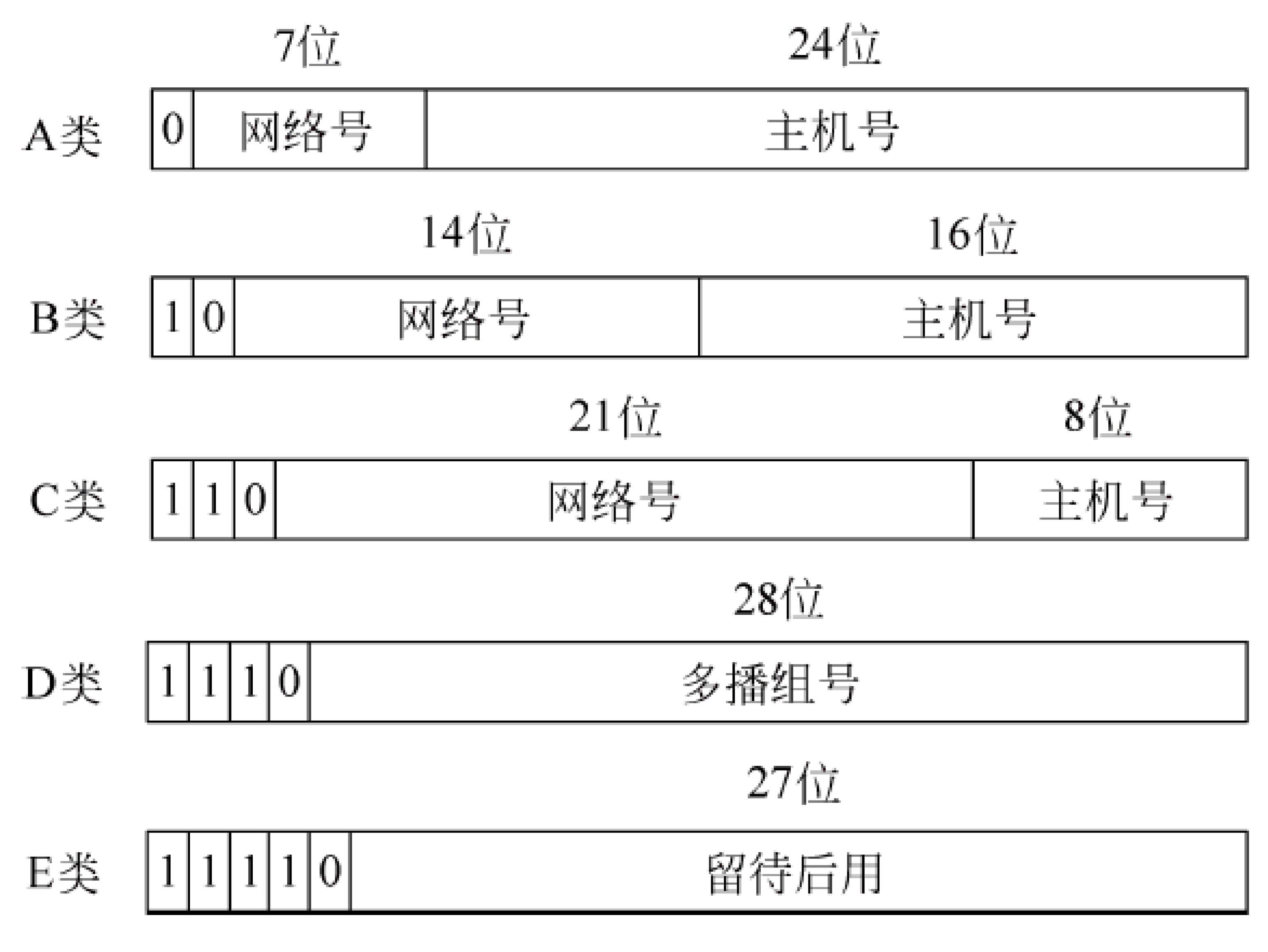


图 2-3　5 类 IP 地址

IP 地址是一个 32 位的二进制数，通常被分割为 4 个“8 位二进制数”(也就是 4 字节)。IP 地址通常用“点分十进制”表示成(a. b. c. d)的形式，其中，a、b、c、d 都是 0～255 的十进制整数。例：点分十进 IP 地址(100. 4. 5. 6)，实际上是 32 位二进制数(01100100. 00000100. 00000101. 00000110)，它是一个 A 类地址。区分各类地址最简单的方法是看它的第一个十进制整数，表 2-2 列出了各类地址的起止范围。

表 2-2　各类 IP 地址的起止范围

类型	范　　围	类型	范　　围
A	0. 0. 0. 0～127. 255. 255. 255	D	224. 0. 0. 0～239. 255. 255. 255
B	128. 0. 0. 0～191. 255. 255. 255	E	240. 0. 0. 0～247. 255. 255. 255
C	192. 0. 0. 0～223. 255. 255. 255		

IP 地址又可分为公有地址和私有地址。

(1) 公有地址(public address)由 Inter NIC(Internet Network Information Center，因特网信息中心)负责，这些 IP 地址分配给注册并向 Inter NIC 提出申请的组织机构，通过它直接访问因特网。

(2) 私有地址(private address)属于非注册地址，专门为组织机构内部使用。

以下列出留用的内部私有地址：

- A 类：10.0.0.0～10.255.255.255
- B 类：172.16.0.0～172.31.255.255
- C 类：192.168.0.0～192.168.255.255

2.2.2　网际控制报文协议

网际控制报文协议（ICMP）是 TCP/IP 协议族的子协议，用于在 IP 主机、路由器之间传递控制报文。控制报文是指网络是否连通、主机是否可达、路由是否可用等网络本身的消息。这些控制报文虽然并不传输用户数据，但是对于用户数据的传递起着非常重要的作用。

1. ICMP 报文的格式

ICMP 报文通常被 IP 层或更高层协议使用，一些 ICMP 报文把差错报文返回给用户进程。ICMP 报文是在 IP 数据报内部被传输的，它的格式如图 2-4 所示。

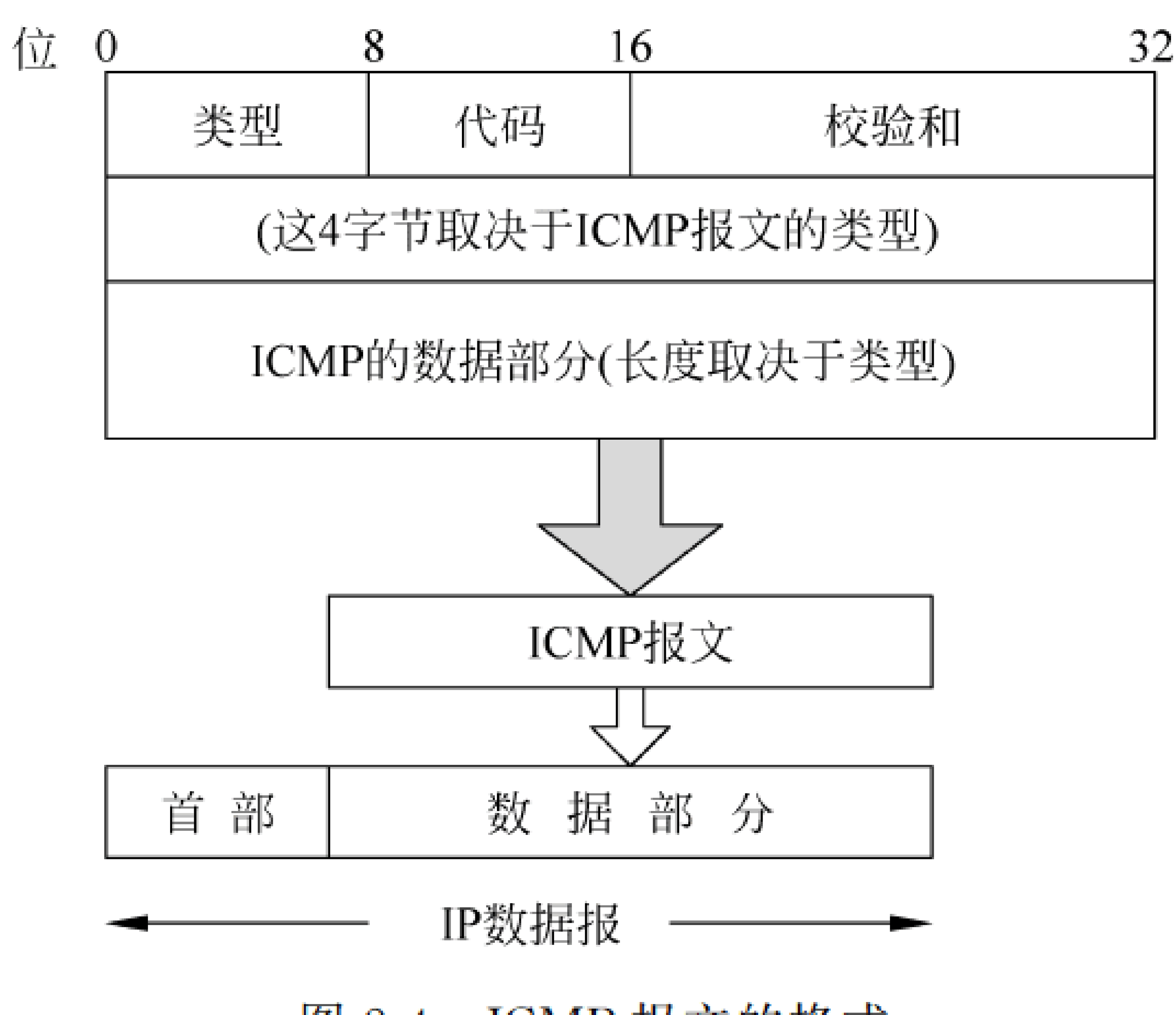


图 2-4　ICMP 报文的格式

ICMP 报文的前 4 字节是统一的格式，共有三个字段，即类型、代码和校验和，接着的 4 字节的内容与 ICMP 的类型有关，最后面是数据字段，其长度取决于 ICMP 的类型。表 2-3 给出了几种常用的 ICMP 报文类型。

表 2-3　几种常用的 ICMP 报文类型

ICMP 报文种类	类型的值	ICMP 报文的类型
差错报告报文	3	终点不可达
	4	源点抑制
	5	改变路由
	11	时间超过
	12	参数问题
询问报文	8 或 0	回送请求或回答
	13 或 14	时间戳请求或回答

2. ICMP 的应用实例

ICMP 的一个重要应用就是分组网间探测 PING（Packet InterNet Groper），用来测试两个主机之间的连通性。PING 使用了 ICMP 回送请求与回送回答报文。PING 是应用层

直接使用网络层 ICMP 的一个例子，它没有通过传输层的 TCP 或 UDP。

图 2-5 给出了从哈尔滨的一台主机到搜狐网的 Web 服务器的连通性的测试结果。主机一连发出了 4 个 ICMP 回送请求报文，如果 Web 服务器正常工作而且响应这个 ICMP 回送请求报文，那么它就发回 ICMP 回送回答报文。由于往返的 ICMP 报文上都有时间戳，因此很容易得出往返时间。

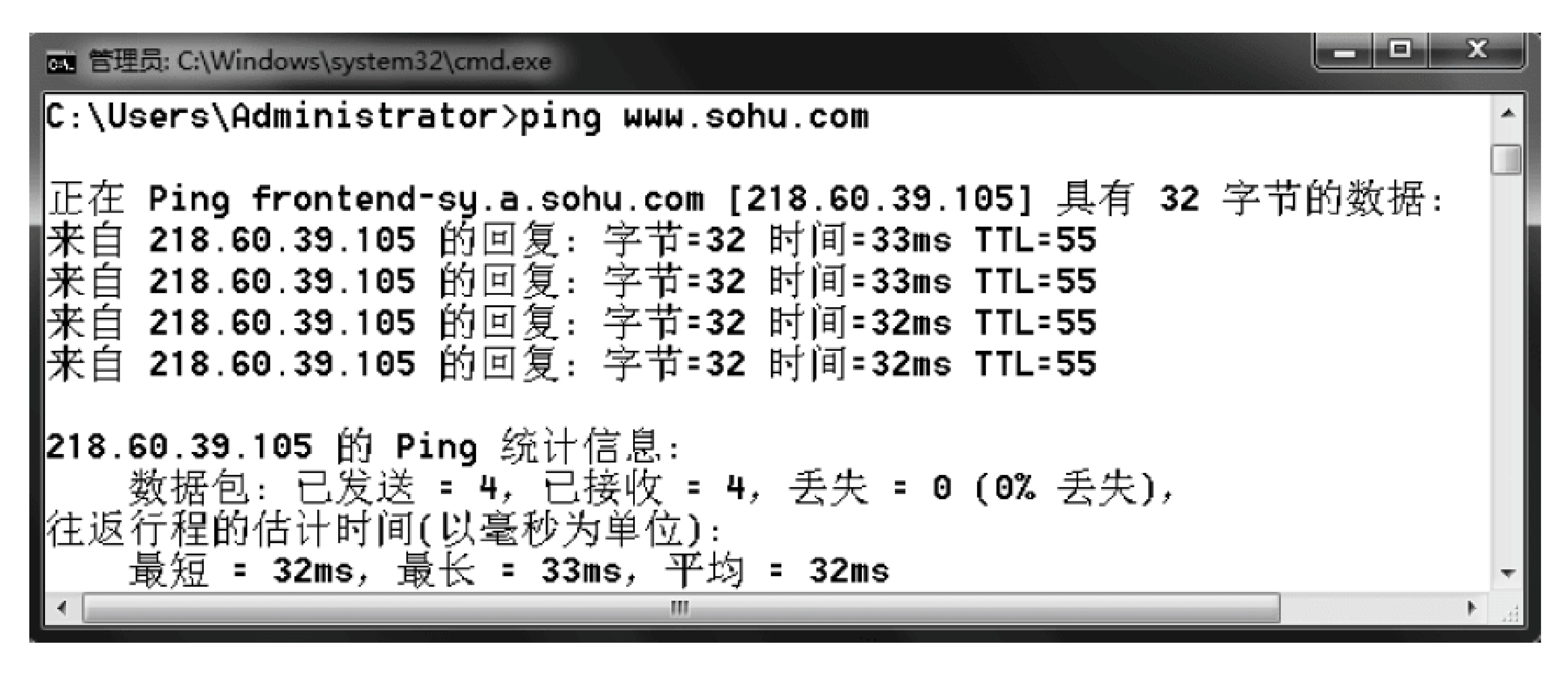


图 2-5　用 ping 测试主机的连通性

2.2.3　地址解析协议

MAC 地址是计算机最终能够识别的物理地址，当发送方计算机发送数据时，将网络连接设备源 MAC 地址和目的 MAC 地址分别封装到帧的源 MAC 和目的 MAC 位，然后将其发送到网络介质上。接收方计算机通过查看帧的目的地址位填写的 MAC 地址，来判断是否和自己的 MAC 地址一致，如果一致，则将其复制，去掉封装并传递到上层应用程序；如果不一致，则网卡丢弃该数据帧。而通信时由于 MAC 地址随硬件随机分布，不易记忆和使用，人们一般使用更容易记忆的 IP 地址进行通信，但是我们指定的 IP 地址必须转化成计算机识别的 MAC 地址才能通信，ARP 就是用于解决这个问题的协议，地址解析（address resolution）是主机在发送帧前将目标 IP 地址转换成目标 MAC 地址的过程。图 2-6 说明了 ARP 的作用。

IP地址 ⟹ ARP ⟹ MAC地址

图 2-6　ARP 协议的作用

1. ARP 工作原理

ARP 解析地址过程如下。

（1）发送方计算机首先检查自己的 ARP 缓存是否有对应的 IP 和 MAC 地址映射的条目：如果有，则找到 MAC 地址，发送数据；如果没有，则需要进一步解析。

（2）发送方发送广播，向所有设备询问该 IP 地址对应的 MAC 地址。对应 IP 地址的计算机回应广播，向发送方发送对应自己 IP 地址和 MAC 地址的映射记录，并且接收方同时将发送方的 IP 地址对应 MAC 地址的映射保留在自己的 ARP 缓存中。

（3）发送方收到 ARP 的回应后，将其保留在自己的 ARP 缓存中，以便下次使用。同时将得到的 MAC 地址封装到帧的目的地址位置，将其发送到网络介质中。

下面举例来解释 ARP 工作过程，如图 2-7 所示。主机 A 要向本局域网内的主机 B 发送 IP 数据报时，首先在其 ARP 高速缓存中查看有无主机 B 的 IP 地址，如果有，就在 ARP

高速缓存中查出其对应的 MAC 地址，再把这个 MAC 地址写入 MAC 帧，然后通过局域网把该 MAC 帧发往此硬件地址；如果找不到主机 B 的 IP 地址的项目，主机 A 就会自动运行 ARP，然后按以下步骤找出主机 B 的硬件地址。

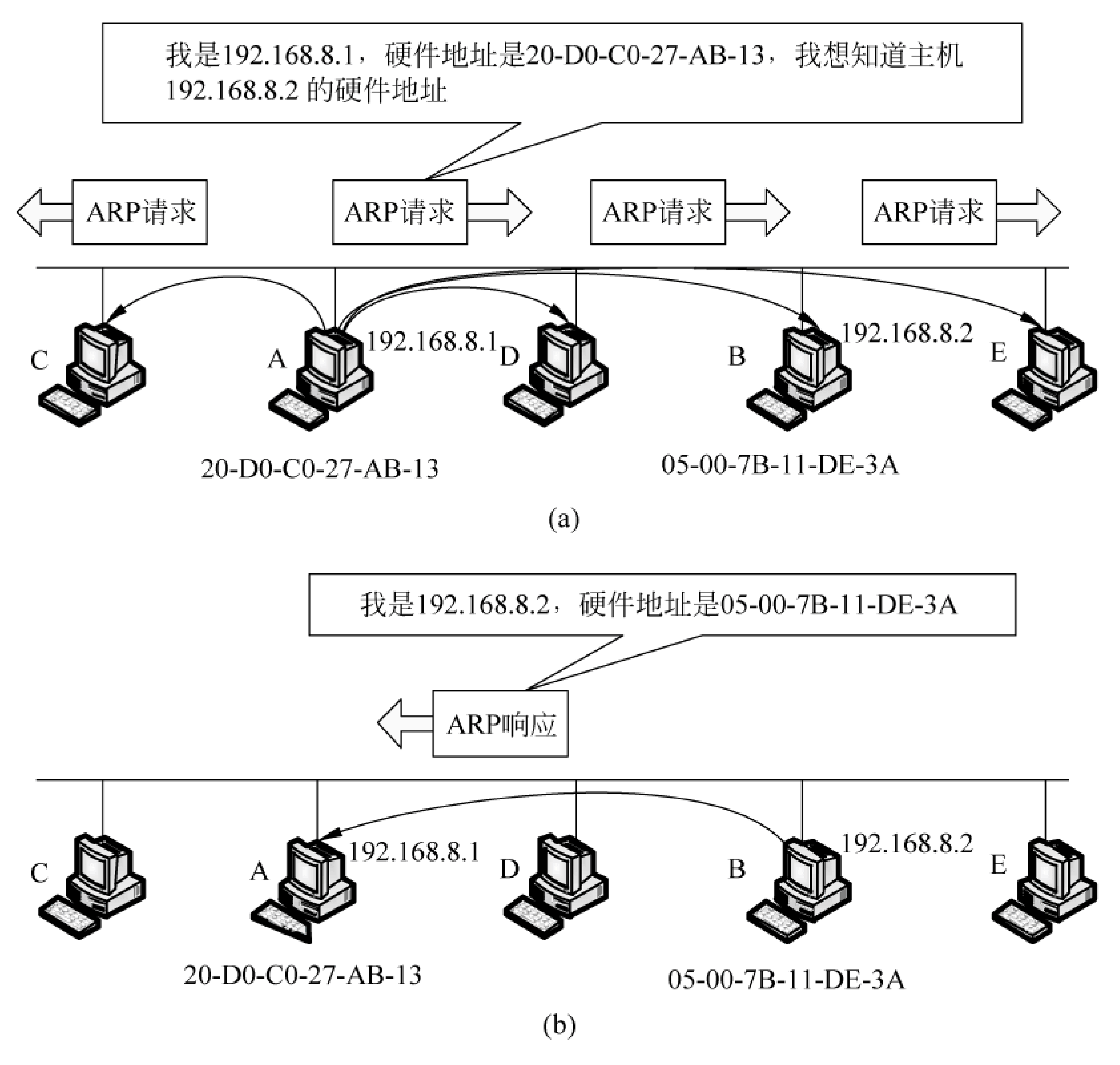


图 2-7　地址解析协议 ARP 的工作过程

（1）ARP 进程在本局域网上广播发送一个 ARP 请求分组，目标 MAC 地址是“FF. FF. FF. FF. FF. FF”（全 1），意思是向同一网段内的所有主机发出询问：“我是 192.168.8.1，硬件地址是 20-D0-C0-27-AB-13，我想知道主机 192.168.8.2 的硬件地址。”图 2-7（a）是主机 A 广播发送 ARP 请求分组的示意图。

（2）本局域网上的所有主机运行的 ARP 进程都收到此 ARP 请求分组。

（3）网络上其他主机不响应 ARP 询问，只有主机 B 接收这个帧，回应“我是 192.168.8.2，硬件地址是 05-00-7B-11-DE-3A”，同时更新自己的 ARP 缓存，见图 2-7（b）。

（4）主机 A 知道了主机 B 的 MAC 地址，它就可以向主机 B 发送信息了。同时，它更新自己的 ARP 缓存，下次再发送信息给 B 时，直接从 ARP 缓存表里查找即可。

2. ARP 提高效率措施

为进一步提高效率，ARP 还采用了如下措施。

（1）高速缓存技术：主机保存已知的 ARP 表项，当收到目的主机的 ARP 应答时将其中的信息加入 ARP 表中。主机发送信息时，先查询 ARP 表，若未找到目的主机的 MAC 地址则用 ARP 协议解析地址。每个表项设置一个计时器，超时即自动删除，以保证表项的有效性。

（2）主机 A 发送 ARP 请求时，包含了自己的 IP 地址和物理地址的映射，而且 ARP 请

求是以广播形式发送出去的，所以包括目的主机在内的网络中的所有主机都会收到此信息，可将此信息保存下来，以备下次使用。

(3) 每台主机启动时广播自己的 IP 地址和 MAC 地址的映射关系，以尽量避免其他主机对它进行 ARP 请求。

3. ARP 缓存表查看方法

ARP 缓存表是可以查看的，也可以添加和修改。在 Windows 系统下，可使用“arp -a”命令观察主机的 ARP 缓存表。图 2-8 中演示查看 ARP 缓存表。

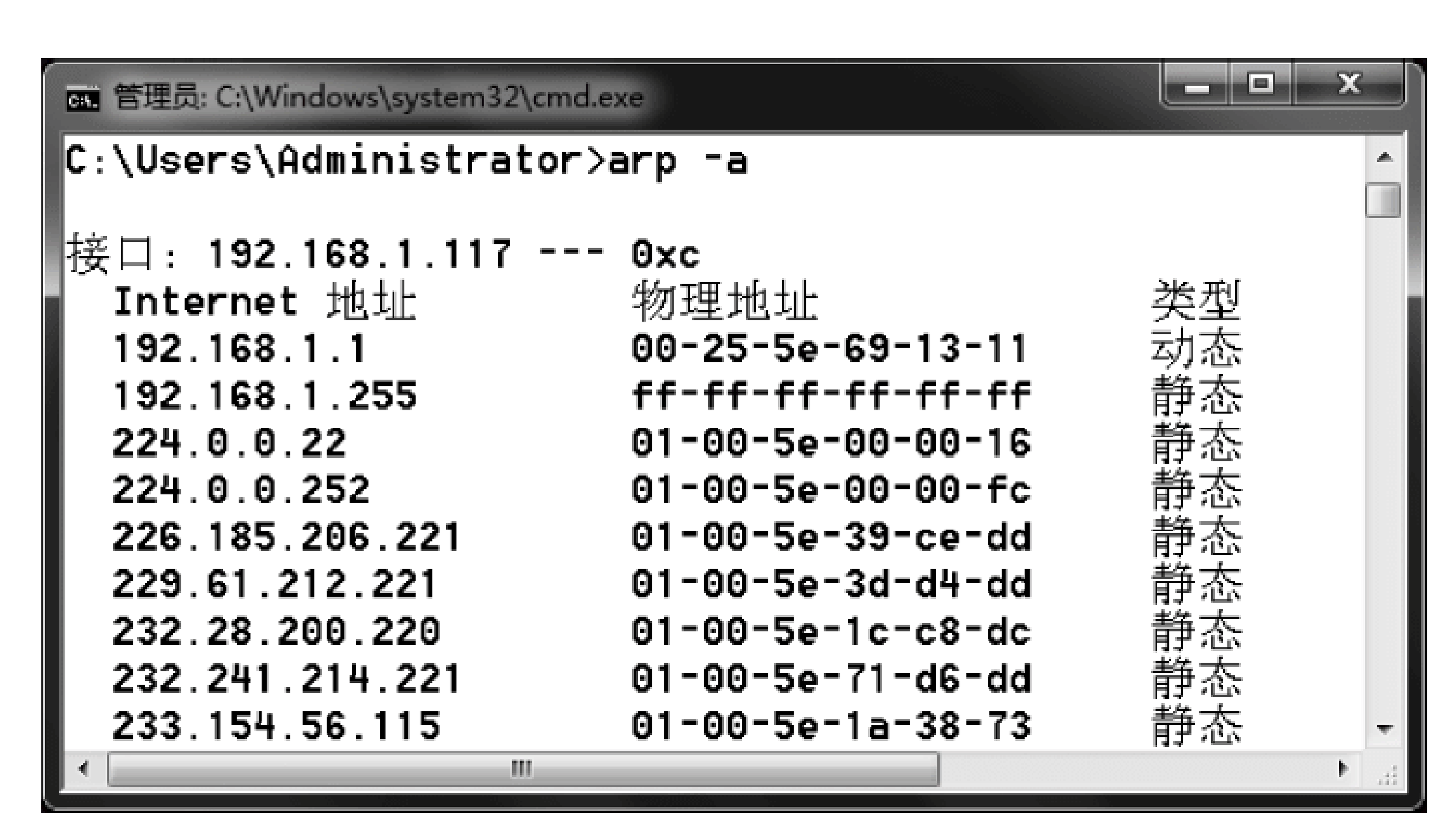


图 2-8　查看 ARP 缓存表

用“arp -d”命令可以删除 ARP 表中所有的内容；用“arp -d ＋空格＋ <指定 IP 地址>”可以删除指定 IP 所在行的内容；用“arp -s”可以手动在 ARP 表中指定 IP 地址与 MAC 地址的对应，类型为 static(静态)，此项存在硬盘中，而不是缓存表，计算机重新启动后仍然存在，且遵循静态优于动态的原则，所以这个设置不对，可能导致无法上网。

2.2.4　传输控制协议

TCP 可以提供面向连接的、可靠的、点到点的全双工传输。

(1) TCP 是面向连接的传输层协议。应用程序在使用 TCP 协议之前，必须先建立连接，在传送数据完毕后，必须释放已建立的 TCP 连接。

(2) TCP 提供可靠交付的服务。即通过 TCP 连接传送的数据，无差错、不丢失、不重复，并且按序到达。

(3) 每一条 TCP 连接只能有两个端点，每一条 TCP 连接只能是点对点的。

(4) TCP 提供全双工通信，即 TCP 允许通信双方的应用进程在任何时候都能发送数据。

1. TCP 首部格式

TCP 报文段首部的前 20 字节是固定的，后面有 $4N$ 字节是根据需要而增加的选项(N 是整数)，因此，TCP 首部的最小长度是 20 字节，如图 2-9 所示。

(1) 源端口和目的端口：各占 2 字节，分别写入源端口号和目的端口号。

(2) 序号：占 4 字节，序号范围是[0，$2^{32}-1$]，共 2^{32}(即 4 284 967 296)个序号，当序号增加到 $2^{32}-1$ 后，下一个序号就又回到 0。

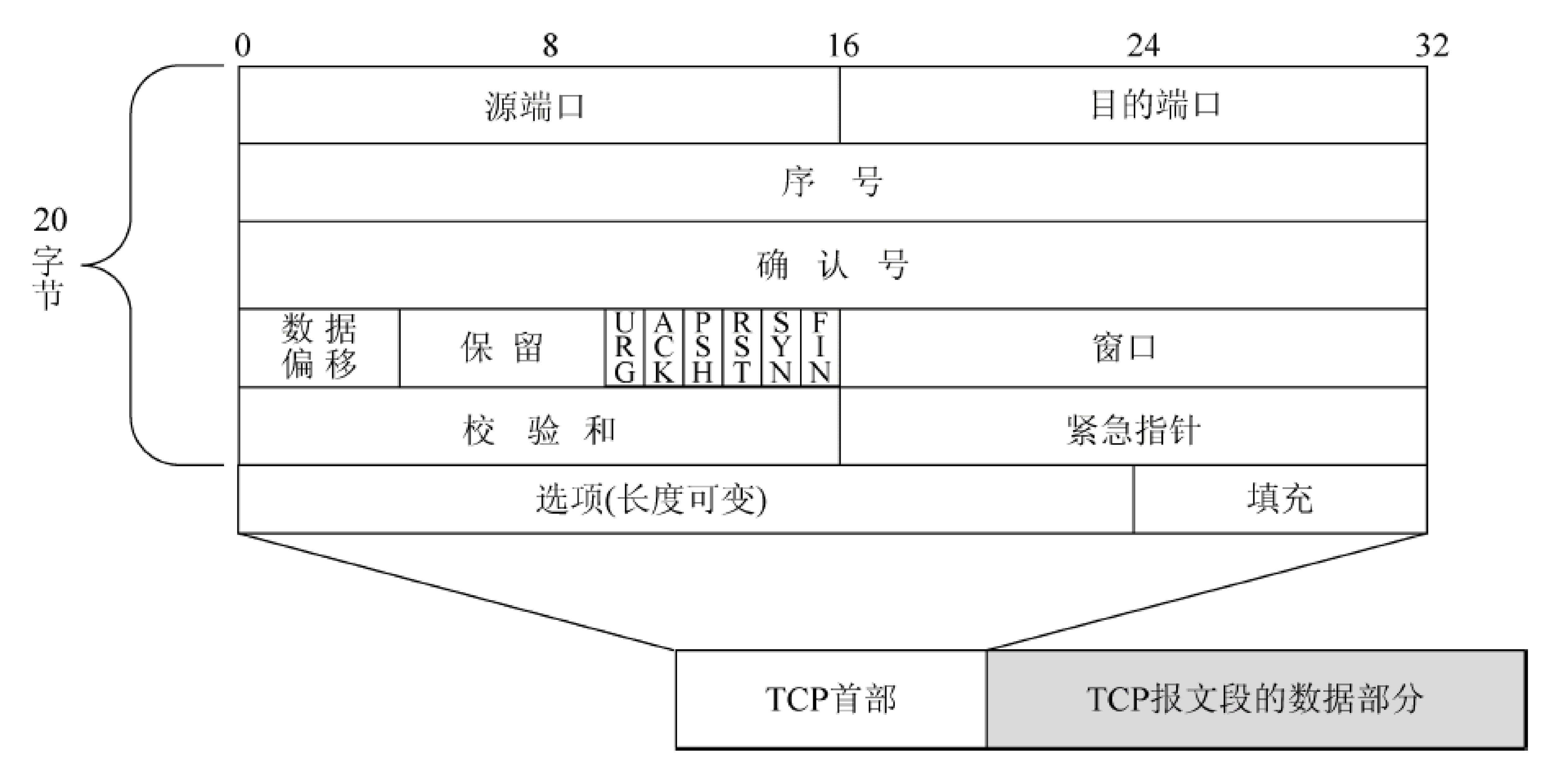


图 2-9 TCP 首部格式

(3) 确认号：占 4 字节，是期望收到对方下一个报文段的第一数据字节的序号。

(4) 数据偏移：占 4 位，它指出 TCP 报文段的数据起始处距离 TCP 报文段的起始处有多远。

(5) 保留：占 6 位，保留为今后使用，但目前应置为 0。

(6) 紧急 URG：当 URG＝1 时，表明紧急指针字段有效，这时要与首部中紧急指针字段配合使用。

(7) 确认 ACK：当 ACK＝1 时，确认号字段才有效，TCP 规定，在连接建立后所有传送的报文段都必须把 ACK 置 1。

(8) 推送 PSH：当 PSH＝1 时，表示以最快的速度传输数据。

(9) 复位 RST：当 RST＝1 时，表明 TCP 连接中出现严重差错，必须释放连接，然后再重新建立传输连接。

(10) 同步 SYN：在连接建立时用来同步序号，当 SYN＝1 时，表示这是一个连接请求或连接接受报文。

(11) 终止 FIN：用来释放一个连接，当 FIN＝1 时，表明从发送方发出的此报文段的数据已发送完毕，并要求释放传输连接。

(12) 窗口：占 2 字节，窗口值是$[0, 2^{16}-1]$之间的整数，窗口指的是发送本报文段的一方的接收窗口。窗口值告诉对方，从本报文段首部中的确认号算起，接收方目前允许对方发送的数据量。

(13) 校验和：占 2 字节，这个校验和与 IP 的校验和有所不同，它不仅对头数据进行校验还对内容进行校验。

(14) 紧急指针：占 2 字节，它指出本报文段中的紧急数据的字节数。

(15) 选项：长度可变，最长可达 40 字节。当没有使用选项时，TCP 的首部长度是 20 字节。

2. TCP 工作原理

TCP 是面向连接的协议，传输连接是用来传送 TCP 报文的，TCP 传输连接的建立和释放是每一次面向连接的通信中必不可少的过程。TCP 在建立连接时需要 3 次确认，俗称

“三次握手”，在断开连接时需要 4 次确认，俗称“四次握手”。

1）TCP 的连接建立

图 2-10 给出了 TCP 的建立连接的过程。假定主机 A 运行的是 TCP 客户程序，而服务器 B 运行 TCP 服务器程序。

三次握手首先要求对本次连接的所有报文进行编号，取一个随机值作为初始序号。由于序号域足够长，可以保证序号循环一周时使用同一序号的旧报文早已传输完毕，网络上也就不会出现关于同一连接、同一序号的两个不同报文。在三次握手的第一次握手中，A 首先向 B 发出连接请求报文段，这时首部中的同步位 SYN＝1，同时选择一个初始序号 seq＝x。在第二次握手中，B 接收到请求连接报文段后，如果同意建立连接，即向 A 发送确认，确认报文段中 SYN 位和 ACK 位都置 1，确认号是 ack＝x＋1，同时也为自己选择一个初始序号 seq＝y。在第三次握手中，当 A 收到 B 的确认后，还要向 B 发出确认，确认号是 ack＝y＋1，而自己的序号是 seq＝x＋1，这时，TCP 连接已经建立，A 和 B 就可以进行数据传送了。

2）TCP 的连接释放

TCP 连接释放过程比较复杂，如图 2-11 所示。

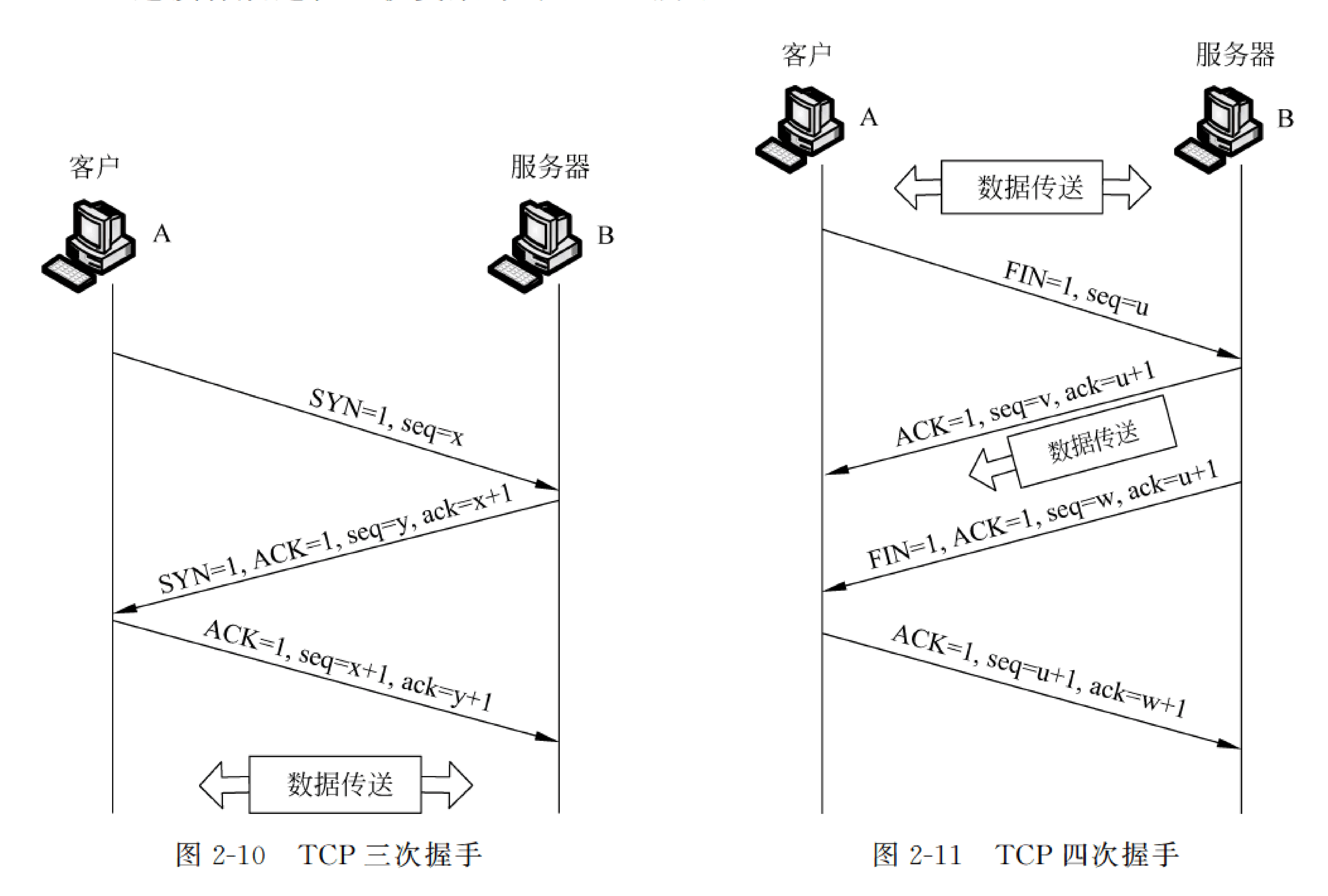


图 2-10　TCP 三次握手　　　图 2-11　TCP 四次握手

在四次握手中，第一次握手，A 的应用进程先向 TCP 发出连接释放报文段，并停止再发送数据，主动关闭 TCP 连接。A 的释放报文段首部的 FIN 置 1，其序号是 seq＝u，它等于前面已传送过的数据的最后一个字节的序号加 1，这时 A 等待 B 的确认。第二次握手，B 收到连接释放报文段后即发出确认，确认号是 ack＝u＋1，而这个报文段自己的序号是 v，等于 B 前面已传送过的数据的最后一个字节的序号加 1，这时的 TCP 连接处于半关闭状态，即 A 已经没有数据要发送了，但 B 若发送数据，A 仍要接收，也就是说，从 B 到 A 的这个方向的连接并未关闭，A 收到来自 B 的确认后，等待 B 发出的连接释放报文段。第三次握手，B 发

出连接释放报文段，报文段首部的 FIN 和 ACK 都置 1，序号 seq＝w（在半关闭状态 B 可能又发送了一些数据），B 还必须重复上次已发送过的确认号 ack＝u＋1，这时 B 等待 A 的确认。第四次握手，A 在收到 B 的连接释放报文段后，必须对此发出确认，在确认报文段中把 ACK 置 1，确认号 ack＝w＋1，而自己的序号是 seq＝u＋1。

2.2.5 用户数据报协议

UDP 可以提供面向无连接的，不可靠的，支持点对点、点对多点的快速传输。

（1）UDP 是无连接的，即发送数据之前不需要建立连接，因此减少了开销和发送数据之前的时延。

（2）UDP 不保证可靠交付，使用尽最大努力交付。

（3）UDP 支持一对一、一对多、多对一和多对多的交互通信。

UDP 有两个字段，数据字段和首部字段。首部字段很简单，只有 8 字节，如图 2-12 所示，由 4 个字段组成，每个字段的长度都是 2 字节。各字段的意义如下。

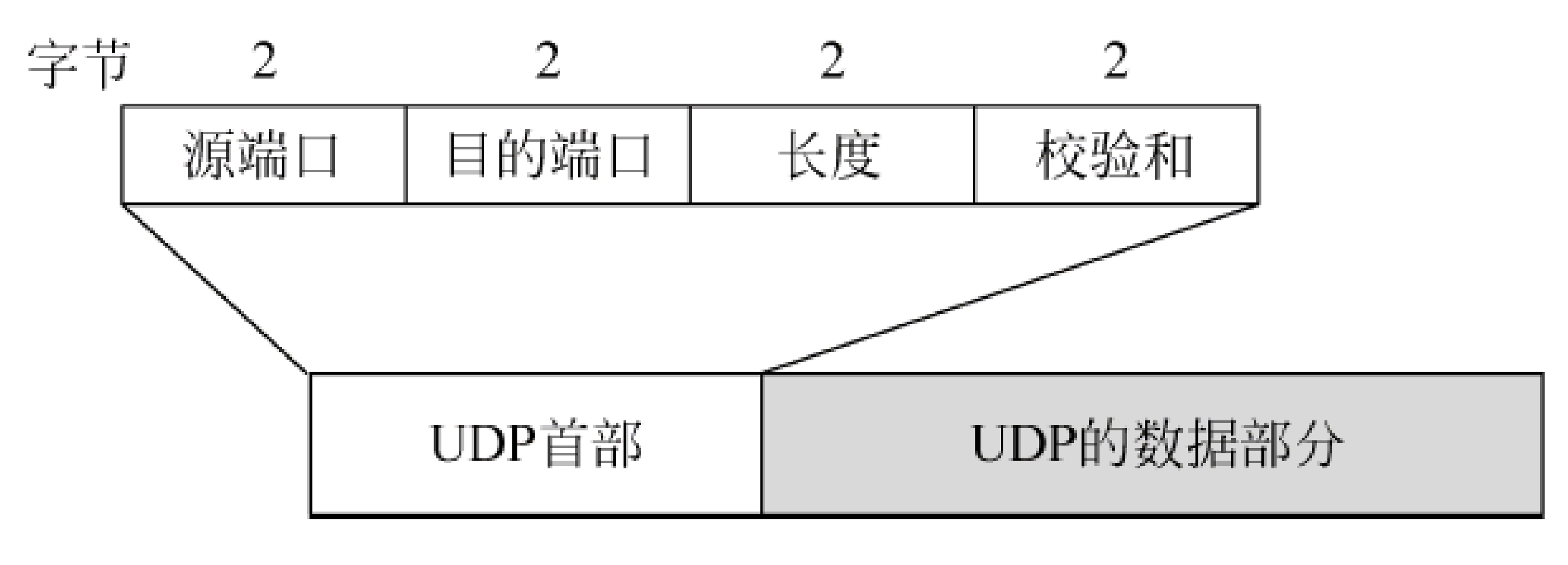


图 2-12　UDP 的首部格式

（1）源端口：写入源端口号，在需要对方回信时选用，不需要时可用全 0。

（2）目的端口：写入目的端口号。

（3）长度：UDP 用户数据报的长度，其最小值是 8（仅有首部）。

（4）校验和：检测 UDP 用户数据报在传输中是否有错。

2.3 TCP/IP 层次安全性

网络体系结构设计目标是实现全世界主机互联互通，所以在设计时只注重了“互联”，而忽略了“安全”，下面分别讨论 TCP/IP 每一层次的安全性问题。

2.3.1 网络接口层安全

网络接口层对应 OSI 参考模型的物理层和数据链路层。

1. 物理安全

物理层的安全主要指网络设施以及线路的安全，主要包括环境安全、电源系统安全、设备安全和通信线路安全。

1）环境安全

计算机网络通信系统的运行环境应按照国家有关标准设计实施，应具备消防报警、安全照明、不间断供电、温湿度控制系统和防盗报警，以保护系统免受水、火、有害气体、地震、静电等的危害。

2）电源系统安全

电源是所有电子设备正常工作的能量源泉，在信息系统中占有重要地位。电源安全主要包括电力能源供应、输电线路安全、保持电源的稳定性等。

3）设备安全

要保证硬件设备随时处于良好的工作状态，建立健全使用管理规章制度，建立设备运行日志。同时注意保护存储媒体的安全性，包括存储媒体自身和数据的安全。存储媒体自身的安全主要是安全保管、防盗、防毁和防霉；数据安全是指防止数据被非法复制和非法销毁。

4）通信线路安全

通信设备和通信线路装置的安装要稳固牢靠，具有一定对抗自然因素和人为因素破坏的能力，包括防止电磁信息的泄漏、线路截获，以及抗电磁干扰。

2. 网络监听

网络监听原本是网络管理员使用一些管理工具，监视网络的状态、数据的流动以及网络上传输的信息。但是网络监听工具也是黑客们常用的工具，当信息以明文的形式在网络上传输时，便可以使用网络监听的方式来获得网络上传输的敏感信息。网络监听可以在网上的任何一个位置实施，如局域网中的一台主机、网关上或远程网的调制解调器之间等。

1）网络监听原理

所谓“监听”技术，就是在互相通信的两台计算机之间通过技术手段插入一台可以接收并记录通信内容的设备，以最终实现对通信双方的数据记录。例如，如图 2-13 所示，在通信主机 A 和通信主机 B 之间，通过技术手段插入一台监听设备，即可实现监听。但需要注意的是，一般都要求用作监听途径的设备不能造成通信双方的行为异常或连接中断，即监听方不能参与通信中任何一方的通信行为，仅仅是“被动”地接收记录通信数据而不能对其进行篡改，一旦监听方违反这个要求，这次行为就不是“监听”，而是“劫持”了。



图 2-13　监听技术原理

2）网络监听实现条件

实现监听要求监听设备的物理传输介质与被监听设备的物理传输介质存在直接联系，或者数据包能经过路由选择到达对方，即存在逻辑上的三方连接。

能实现监听条件的情况如下：

（1）监听方与通信方是位于同一物理网络的，如局域网。

（2）监听方与通信方存在路由或接口关系，例如通信双方有同一网关等。

3）共享式局域网内的监听

（1）什么是共享式局域网。

所谓“共享式”局域网，指早期采用集线器（HUB）作为网络连接设备的传统局域网的结

构，如图 2-14 所示。在这个结构里，所有机器都是共享同一条传输线路的，集线器没有端口的概念，它的数据发送方式是“广播”，集线器接收到相应数据时是单纯地把数据往它所连接的每一台设备线路上发送。

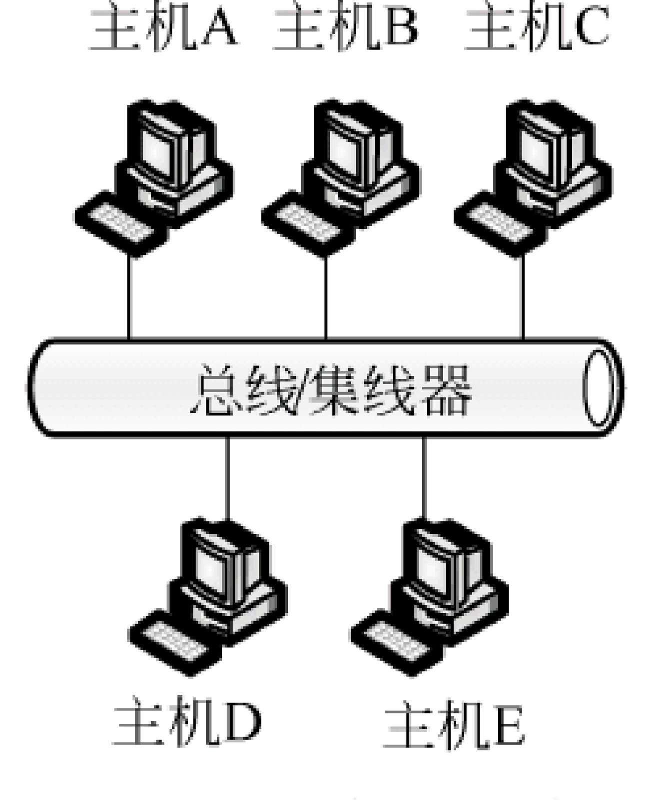


图 2-14　共享式局域网

（2）共享式局域网工作过程。

共享式局域网协议的工作方式是将要发送的数据包发往连接在一起的所有主机，在包头中包括应该接收数据包的主机的正确地址。在共享式局域网中，填写了物理地址的帧从网络接口即从网卡中发送出去，传送到物理的线路上，当发送出去的信号到达集线器，由集线器再发向连接在集线器上的每一条线路，于是，在物理线路传输的数字信号也就到达连接在集线器上的每一台主机。数字信号到达一台主机的网络接口时，在正常情况下，网络接口读入数据帧，然后进行检查，如果数据帧中携带的物理地址是自己的，或者物理地址是广播地址，将由数据帧交给上层协议软件，即 IP 层软件。也就是说，只有与数据包中目标地址一致的那台主机才能接收数据包，否则就将这个帧丢弃。对于每一个到达网络接口的数据帧，都要通过这个过程。例如，在图 2-14 中，主机 A 发送一条报文给主机 B，所有连接在这个局域网中的计算机都会收到这条报文，但是只有主机 B 才会接收处理这条报文，而其他计算机则会抛弃该报文。

（3）共享式局域网监听的实现。

当主机工作在监听模式下，主机收到的所有的数据帧都将交给上层协议软件处理。也就是说，主机 A 发送报文给主机 B，主机 C、D、E 都接收该报文，不丢弃报文。所以，共享式局域网结构里的数据实际上是没有隐私性的，我们希望网卡会丢弃与自己无关的报文，但实际上它可以不丢弃，只需要来调整网卡（网络接口）的工作模式为混杂模式。

每块网卡基本上都会有以下 4 种工作模式：

- 广播模式（Broadcast）：该模式下的网卡能够接收网络中的广播信息。
- 组播模式（Multicast）：设置在该模式下的网卡能够接收组播数据。
- 直接模式（Unicast）：在这种模式下，只有目的网卡才能接收该数据。
- 混杂模式（Promiscuous）：在这种模式下的网卡能够接收一切通过它的数据，而不管该数据是否是传给它的。

在混杂模式里，网卡对报文中的目标 MAC 地址不进行任何检查而全部接收，这样就造成网卡接收所有路过的数据，监听就是从这里开始的。

4）交换式局域网内的监听

（1）什么是交换式局域网。

作为与“共享式”相对的“交换式”局域网，它的网络连接设备被换成了交换机，如图 2-15 所示。交换机引入了“端口”的概念，它会产生一个地址表用于存放每台与之连接的计算机的 MAC 地址，从此每个网络接口便作为一个独立的端口存在。

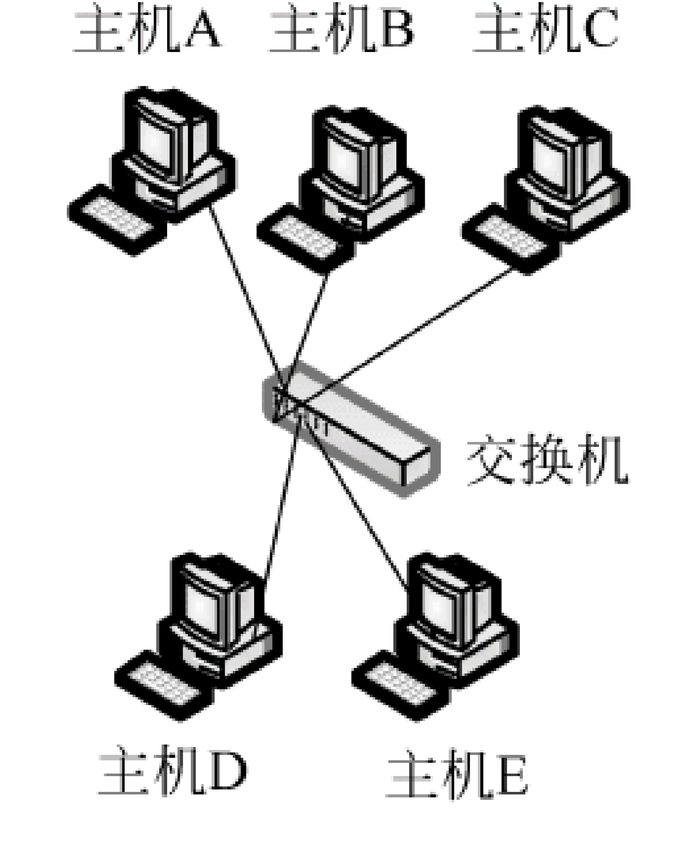


图 2-15　交换式局域网

（2）交换式局域网的工作过程。

在交换式局域网中，除了声明为广播或组播的报文，交换机在一般情况下是不会让其他报文出现类似共享式局域网那样以广播

形式的发送行为，这样即使网卡设置为混杂模式，它也收不到发往其他计算机的数据，因为数据的目标地址会在交换机中被识别，然后有针对性地发往表中所对应地址的端口。例如，在图 2-15 中，主机 A 发送一条报文给主机 B，主机 A 首先将报文发送给交换机，交换机会查看报文中的目的地址，然后交换机查找自己的交换表，根据目的地址与端口的对应关系，直接将报文发送给主机 B。

(3) 交换式局域网监听的实现。

MAC 洪水攻击，就是向交换机发送大量含有虚假 MAC 地址和 IP 地址的 IP 包，使交换机无法处理如此多的信息而引起设备工作异常，即所谓的“失效”模式。在这个模式里，交换机的处理器已经不能正常分析数据报查询地址表了，然后，交换机就会成为一台普通的集线器，毫无选择地向所有端口发送数据，这个行为被称作“泛洪发送”，这样一来攻击者就能监听到所需数据了。

5) 局域网内监听的防御

(1) 从逻辑或物理上对网络分段。

网络分段通常被认为是控制网络广播风暴的一种基本手段，但其实也是保证网络安全的一项措施。其目的是将非法用户与敏感的网络资源相互隔离，从而防止可能的非法监听。

(2) MAC 地址绑定。

虽然利用 ARP 欺骗报文进行的网络监听很难察觉，但它并不是无法防御的。与 ARP 寻址相对的，在一个相对稳定的局域网里，我们可以使用静态 ARP 映射，记录下局域网内所有计算机的网卡 MAC 地址和对应的 IP，然后使用“arp -s IP 地址 MAC 地址”进行静态绑定，这样计算机就不会通过 ARP 广播来找人了，自然不会响应 ARP 欺骗工具发送的动态 ARP 应答包(静态地址的优先度大于动态地址)。

(3) 使用软件防御。

例如 Anti Arp Sniffer，它可以强行绑定本机与网关的 MAC 关系，让伪装成网关获取数据的监听机成为摆设，如果监听者仅仅欺骗了某台计算机，这时就要使用 ARP Watch 了，ARP Watch 会实时监控局域网中计算机 MAC 地址和 ARP 广播报文的变化情况，如果有 ARP 欺骗程序发送虚假地址报文，必然会造成 MAC 地址表不符，ARP Watch 就会弹出来警告用户。

(4) 划分 VLAN。

对网络进行 VLAN 划分也是有效的方法，每个 VLAN 之间都是隔离的，必须通过路由进行数据传输，这个时候 MAC 地址信息会被丢弃，每台计算机之间都是采用标准 TCP/IP 进行数据传输的，即使存在监听工具也无法使用虚假的 MAC 地址进行欺骗。

(5) 使用加密技术。

数据经过加密后，通过监听仍然可以得到传送的信息，但显示的是乱码。使用加密技术的缺点是影响数据传输速度以及使用一个弱加密比较容易被攻破。系统管理员和用户需要在网络速度和安全性上进行折中选择。

2.3.2 网际层协议安全

1. IP 协议安全问题及防护措施

1) IP 窃听

IP 数据报在传递过程中易被攻击者监听、窃取。此种攻击是一种被动的攻击方式，攻

击者并不改变 IP 数据报的内容，但可截取 IP 数据报，解析数据，从而获得数据内容。这种类型的攻击很难被检测，因为攻击过程并不影响 IP 数据报的正确传递。针对这种攻击的防御方法是对 IP 数据报进行加密。

2）IP 地址假冒

高层的 TCP 和 UDP 服务在接收 IP 数据报时，通常假设数据报中的源地址是有效的。事实上，IP 层不能保证数据报一定是从源地址发送的。任意一台主机都可以发送具有任意源地址的 IP 数据报。攻击者可伪装成另一个网络主机，发送含有伪造源地址的数据包以欺骗接收者。针对此种攻击可以通过源地址鉴别机制加以防御。一般来说，认证需要采用高层协议中的安全机制来实现。

3）IP 碎片攻击

在传递过程中，太大的 IP 数据报会被分段。也就是说，大的 IP 数据报会被分成两个或多个小数据报，每个小数据报都有自己的首部，但其数据部分只是大数据报数据的一部分。每个小数据报可以经由不同的路径到达接收方。在传输过程中，每个小数据报可能会继续被分段。当这些小数据报到达接收方时，它们会被重组到一起。攻击者可以发送大量的小数据报来破坏包过滤器的正常工作。

2. ARP 协议安全问题及防护措施

在局域网寻址方式中，一台主机 A 如果要向目标主机 B 发送数据，无论主机 B 在本网段还是在远程网络，这些需要发送出去的数据包中需要 4 种必不可少的地址：(源 IP 地址，源 MAC 地址)+(目的 IP 地址，目的 MAC 地址)。当主机 A 在封装数据包时，自然知道自己的 IP 地址和 MAC 地址，同时还知道目标的 IP 地址，需要得到 B 的 MAC 地址。通过 ARP 协议，主机 A 得到主机 B 的 MAC 地址，并且把 IP 地址与 MAC 地址的对应关系放在缓存表中，以备下一次使用。但要说明的是，因为考虑到主机 B 有更换网卡的可能，所以无论何时当主机 A 再次收到关于主机 B 的 MAC 地址信息，它都将刷新自己的 ARP 缓存表，将新收到的 MAC 地址和主机 B 的 IP 地址对应起来，正因为主机 A 在任何时候收到 ARP 数据包，都将再次更新 ARP 缓存，所以导致了 ARP 欺骗的发生。

如图 2-16 所示，假设局域网内有两台主机 A 和 B 在通信，而主机 C 要作为一个监听者得到这两台主机的通信数据，那么它就必须想办法让自己能插入两台主机之间的数据线路里，而在这种一对一的交换式网络里，主机 C 必须成为一个中间设备才能让数据得以经过它，要实现这个目标，主机 C 就要伪造虚假的 ARP 报文。

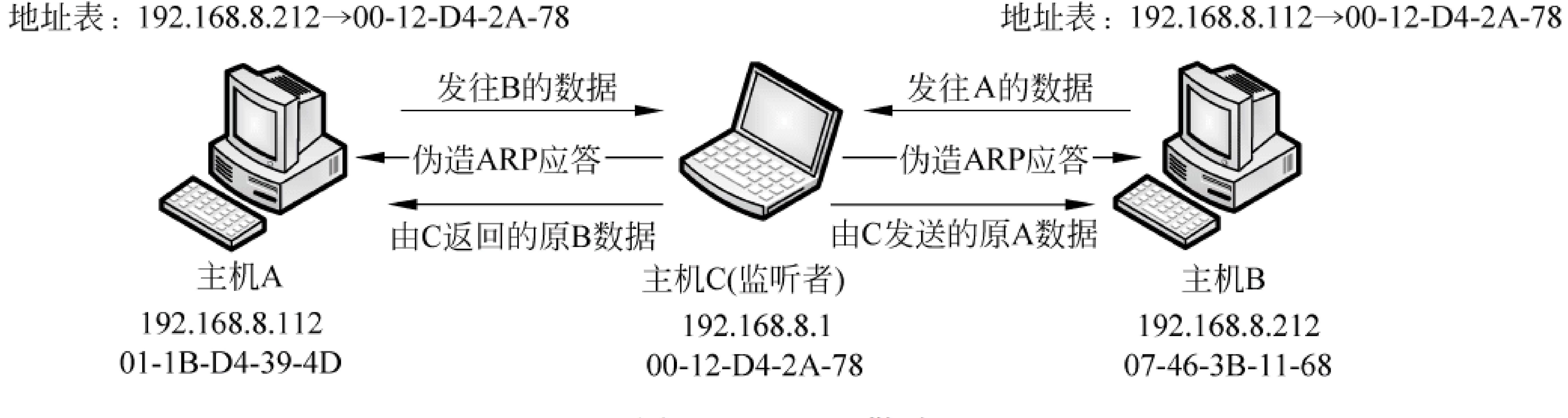


图 2-16　ARP 欺骗

如果现在主机 C 想要窃取网络中的数据，那么这时它就可能向 A 发送一个 ARP 数据包，数据包中声称主机 B 的 MAC 地址已经改变，当主机 A 收到数据包后，得知此消息，就立刻更新原来主机 B 的 MAC 地址，当它要和主机 B 进行通信时，就会在数据包中封装新的 MAC 地址，如果这个 MAC 地址是主机 C 的，那么主机 A 就会把本来要发给主机 B 的数据错误地发给主机 C，被主机 C 监听成功，而主机 C 为了掩人耳目，“看”过数据后，再发给主机 B，从而不影响主机 A 和主机 B 之间的正常通信。

实际上，真实环境里的 ARP 欺骗除了监听主机 A 的数据，通常也会顺便监听主机 B 的数据，只要主机 C 在对主机 A 发送伪装成主机 B 的 ARP 应答包的同时也向主机 B 发送伪装成主机 A 的 ARP 应答包即可，这样它就可作为一个双向代理插入两者之间的通信链路。建立静态 ARP 表，是一种有效抵抗 ARP 欺骗攻击的方法，而且对系统影响不大。

2.3.3 传输层协议安全

1. TCP 安全问题及防护措施

TCP 的三次握手机制给攻击者提供了可以利用的漏洞。TCP 是一个面向连接的协议，即在数据传输之前要首先建立连接，然后再传输数据，当数据传输完毕后释放所建立的连接。攻击者不断向服务器的监听端口发送建立 TCP 连接的请求 SYN 数据包，但收到服务器的 SYN 包后却不回复 ACK 确认信息，每次操作都会使服务器端保留一个半开放的连接，当这些半开放连接填满服务器的连接队列时，服务器便不再接受后续的任何连接请求，这种攻击属于拒绝服务攻击。防御这类攻击的主要思路是在服务器前端部署相应的网络安全设备，比如防火墙设备，以对 SYNFLOOD 攻击数据包进行过滤。

2. UDP 安全问题及防护措施

DoS 攻击是一种常见的 UDP 攻击，而 UDP Flood 攻击又是 DoS 攻击中最普遍的流量型攻击。其攻击原理是，攻击源发送大量的 UDP 小包到攻击目标，目标可以是服务器或者网络设备，使其忙于处理和回应 UDP 报文，使系统资源耗尽，最后导致该设备不能提供正常服务或者直接死机，严重的会造成全网瘫痪。使用 UDP 进行传输的应用层协议之间差异极大，因此不同情况下的 UDP 攻击需要采取不同的防护手段。如果攻击包是大包，则根据攻击包大小设定包碎片重组大小，通常不小于 1500，极端情况下可以考虑丢弃所有 UDP 碎片。当攻击端口为业务端口，根据该业务设置 UDP 最大包以过滤异常流量。当攻击端口为非业务端口，通常通过设置 UDP 连接规则，要求所有去往该端口的 UDP 包必须首先与 TCP 端口建立 TCP 连接，不过这种方法需要借助专业安全设备。

2.3.4 应用层协议安全

1. HTTP 安全问题及防护措施

由于 HTTP 设计之初未进行安全方面的考虑，数据是直接通过明文进行传输的，不提供任何方式的数据加密，因此存在较大的安全缺陷。

(1) 攻击者可以通过网络嗅探工具轻易获得明文的传输数据，从而分析出特定的敏感

信息,如用户的登录口令等。

(2) HTTP 是一种无状态的连接,在传输客户端请求和服务器响应时,唯一的完整性检验就是在报文头部包含了数据传输长度,而未对传输内容进行消息完整性检测,攻击者可以轻易篡改传输数据,发动中间人攻击,因此 HTTP 不适合传输重要信息。

针对 HTTP 的这些安全问题,超文本传输安全协议(Hyper Text Transfer Protocol Secure,HTTPS)在 HTTP 和 TCP 之间增加了安全层来增强安全性,安全层主要通过安全套接层(Secure Sockets Layer,SSL)及其替代协议传输层安全协议 (Transport Layer Security,TLS)实现。与 HTTP 不同,SSL 协议通过 443 端口进行传输,主要包含记录协议(SSL Record Protocol)和握手协议(SSL Handshake Protocol),记录协议确定了对传输层数据进行封装,具体实施加密解密、计算和校验等安全操作。握手协议使用 X. 509 认证,用于验证传送数据,协商加密算法,并利用非对称加密算法进行身份认证和生成会话密钥等操作,从而对通信双方交换的数据加密,保证客户与服务器之间的通信不被攻击者窃听。

HTTPS 协议通过增加安全层,可实现双向身份认证、生成会话密钥、传输数据加密、数据完整性验证和防止数据包重放攻击等安全功能,其主要改进是使用非对称加密算法在不可信的互联网上安全传输用来对称加密的会话密钥,从而建立安全信道,因此很多银行和邮箱等安全级别高的服务都使用 HTTPS 协议。但由于 HTTPS 协议会额外增加握手过程并对数据进行加密,因此会在一定程度上拖慢网页加载速度。

2. DNS 安全问题及防护措施

在正常工作模式下,备份服务器可使用"区转移"来获得域名空间中所属信息的完整备份,黑客也常使用这种方式快速获得攻击目标列表。如果将前向命名和后向命名分离,可能会带来安全问题,黑客若能够掌控部分反向映射树,就能实施欺骗,也就是说,反向记录中可能含有可依赖的那台主机的名称(伪造)。攻击者在发起呼叫之前,会扰乱目标主机中 DNS 响应的高速缓存,当目标主机进行交叉检验时,验证结果似乎是成功的,但此时黑客却已经获得了访问权。另外,黑客采用呼叫响应的方式来淹没目标的 DNS 服务器,可使其陷入混乱,此类攻击案例十分常见,黑客只需用非常简单的程序就可以捣毁 DNS 的高速缓存。

虽然我们无法阻止黑客对 DNS 的不断攻击,但是可以通过采取相应的措施加以控制,如可以对授权的第二级服务器限制"区转移"功能的使用。DNSsec 是 DNS 的安全扩展,由 IETF 提供的一系列 DNS 安全认证机制组成,它可以对 DNS 记录进行数字签名,是消除欺骗性 DNS 记录的最简便的方法。当某个区的所有者有不良动机时,DNSsec 就会签署一个欺骗性的记录,进而可以有效防止此类欺骗。此外,对域的签名可以离线进行,从而降低了域签名私钥泄露的风险。虽然 DNSsec 对付以上欺骗攻击很有效,但也有一些不足之处,所以它迄今还没有成为主流的 DNS 查询方式。

2.4 网络安全协议

安全协议(Security Protocol)又称密码协议,是建立在密码体制基础上的一种交互通信协议,它运用密码算法和协议逻辑来实现认证和密钥分配等目标。安全协议可用于保障计

算机网络信息系统中信息的秘密安全传递与处理,确保网络用户能够安全、方便、透明地使用系统中的密码资源。

2.4.1 网络各层相关的安全协议

运行在网络各层次的相关安全协议及其内容如表 2-4 所示。

表 2-4 网络各层相关的安全协议

层次	相关协议	描述
应用层	S-HTTP	Secure-Hyper Text Protocol 是为保证 WWW 的安全,由 EIT(Enterprise Integration Technology Corp)开发的协议,利用 MIME 基于语言本进行加密、报文认证及密钥分发等
	SSH	Secure Shell 是对 BSD 系统的 UNIX 的 rsh/rlogin 等的 r 命令加密而采用的安全技术
	SSL-telent SSL-SMTP SSL=POP3	以 SSL 分别对 Secure Sockets Layer-telnet、SSL-Simple Mail Transfer Protocol 和 SSL-Post Office Protocol Version3 等的应用进行加密
	PET	Privacy Enhanced Telnet 使 telnet 具有加密功能,是在远程登录时对连接本身进行加密的方式
	S/MIME	Secure/Multipurpose Internet Mail Extensions 是利用 RSA Data Secure 公司提出的 PKCS(Public-Key-Cryptography Standards)加密技术实现的 MIME 的安全功能
	PGP	Pretty Good Privacy 是 Philip Zimmermann 开发的带加密和签名功能的邮件系统
传输层	SSL	Secure Sockets Layer 在 Web 服务器和浏览器之间进行加密
	TLS	Transport Layer Security 是将 SSL 通用化的协议
	Socks v5	防火墙及 VPN 用的数据加密及认证协议
网络层	IPSec	Internet Protocol Security Protocol,以 IPSec 通信时通信对象的密钥交换方式使用 IKE(Internet Key Exchange)
数据链路层	PPTP	Point to Point Tunneling Protocol
	L2F	Layer2 Forwarding
	L2TP	Layer2 Tunneling Protocol 综合了 PPTP 和 L2F 协议

2.4.2 IPSec 协议

IPSec(IP Security Protocol,IP 安全协议)在 IPv6 的制定过程中产生,用于提供 IP 层的安全性。由于所有支持 TCP/IP 的主机在进行通信时都要经过 IP 层的处理,所以提供了 IP 层的安全性就相当于为整个网络提供了安全通信的基础。鉴于 IPv4 的应用仍然很广泛,后来在 IPSec 的制定中也增添了对 IPv4 的支持。

IPSec 标准最初由 IETF 于 1995 年制定,但由于其中存在一些未解决的问题,从 1997 年开始 IETF 又开展了新一轮的 IPSec 标准的制定工作,1998 年 11 月,主要协议已经基本制定完成。由于这组新的协议仍然存在一些问题,IETF 将来还会对其进行修订。

IPSec 涉及的一系列 RFC 标准文档如下。

- RFC 2401：IPSec 系统结构
- RFC 2402：认证首部协议(AH)
- RFC 2406：封装净荷安全协议(ESP)
- RFC 2408：因特网安全联盟和密钥管理协议(ISAKMP)
- RFC 2409：因特网密钥交换协议(IKE)
- RFC 2764：基本框架文档
- RFC 22631：Diffie-Hellman 密钥协商方案
- SKEME

IPSec 是一组开放标准集,它们协同地工作来确保对等实体之间的数据机密性、数据完整性以及数据认证。这些对等实体可能是一对主机或是一对安全网关(路由器、防火墙、VPN 集中器等),或者它们可能在一个主机和一个安全网关之间,就像远程访问 VPN 的情况。IPSec 能够保护对等实体之间的多个数据流,并且一个单一网关能够支持不同的成对的合作伙伴之间的多条并发安全 IPSec 隧道。

IPSec 保护涉及 5 个主要组件。

(1) 安全协议：IP 数据报保护机制。验证头(Authentication Header,AH)对 IP 包进行签名并确保其完整性。数据包的内容没有加密,但是可以向接收者保证包的内容尚未更改,还可以向接收者保证包已由发送者发送。封装安全载荷(Encapsulating Security Payload,ESP)对 IP 数据进行加密,因此在包传输过程中会遮蔽内容。

(2) 安全关联数据库(Security Associations Database,SADB)：将安全协议与 IP 目标地址和索引号进行关联的数据库。索引号称为安全参数索引(Security Parameter Index,SPI),安全协议、IP 目标地址和 SPI 三个元素唯一标识合法的 IPSec 包。此数据库确保到达包目的地的受保护包可由接收者识别。接收者还可使用数据库中的信息解密通信、检验包未曾受到更改、重新组装包并将包发送到其最终目的地。

(3) 密钥管理：针对加密算法和 SPI 生成和分发密钥。

(4) 安全机制：用于保护 IP 数据报中的数据的验证和加密算法。

(5) 安全策略数据库(Security Policy Database,SPD)：用于指定要应用到包的保护级别的数据库。SPD 过滤 IP 通信来确定应该如何处理包。包可能被废弃,可以毫无阻碍地进行传送,也可以受到 IPSec 的保护。对于外发包,SPD 和 SADB 确定要应用的保护级别。对于传入包,SPD 帮助确定包的保护级别是否可接受。如果包受 IPSec 保护,将在对包进行解密和验证之后参考 SPD。

IPSec 将安全机制应用于发往 IP 目标地址的 IP 数据报。接收者使用其 SADB 中的信息来检验到达的包是否合法并对其进行解密。应用程序也可以调用 IPSec,以便在每个套接字级别将安全机制应用于 IP 数据报。

1. IPSec 的工作原理

IPSec 的工作原理类似于包过滤防火墙,可以把它看作是包过滤防火墙的一种扩展。IPSec 通过查询安全策略数据库(Security Policy Database,SPD)决定如何对接收到的 IP 数据报进行处理。但是 IPSec 与包过滤防火墙不同,它对 IP 数据报的处理方法除了丢弃和直接转发(绕过 IPSec)外,还可以对数据包进行 IPSec 处理。正是这种新增添的处理方法,使

VPN 提供了比包过滤防火墙更高的安全性。

进行 IPSec 处理意味着对 IP 数据报进行加密和认证。包过滤防火墙只能控制来自或去往某个站点的 IP 数据报的通过，即它可以拒绝来自某个外部站点的 IP 数据报访问内部网络资源，也可以拒绝某个内部网络用户访问某些外部网站。但是包过滤防火墙不能保证自内部网络发出的数据包不被截取，也不能保证进入内部网络的数据包未经篡改。只有在对 IP 数据报实施了加密和认证后，才能保证在公用网络上传输数据的机密性、认证性和完整性。

IPSec 既可以对 IP 数据报只进行加密或认证，也可以同时实施加密和认证。但无论是进行加密还是进行认证，IPSec 都有两种工作模式：一种是传输模式；另一种是隧道模式。

1）传输模式

采用传输模式时，IPSec 只对 IP 数据报的净荷进行加密或认证。此时，封装数据包继续使用原 IP 头部，只对 IP 头部的部分域进行修改，而 IPSec 协议头部插入到原 IP 头部和传输层头部之间。IPSec 传输模式如图 2-17 所示。

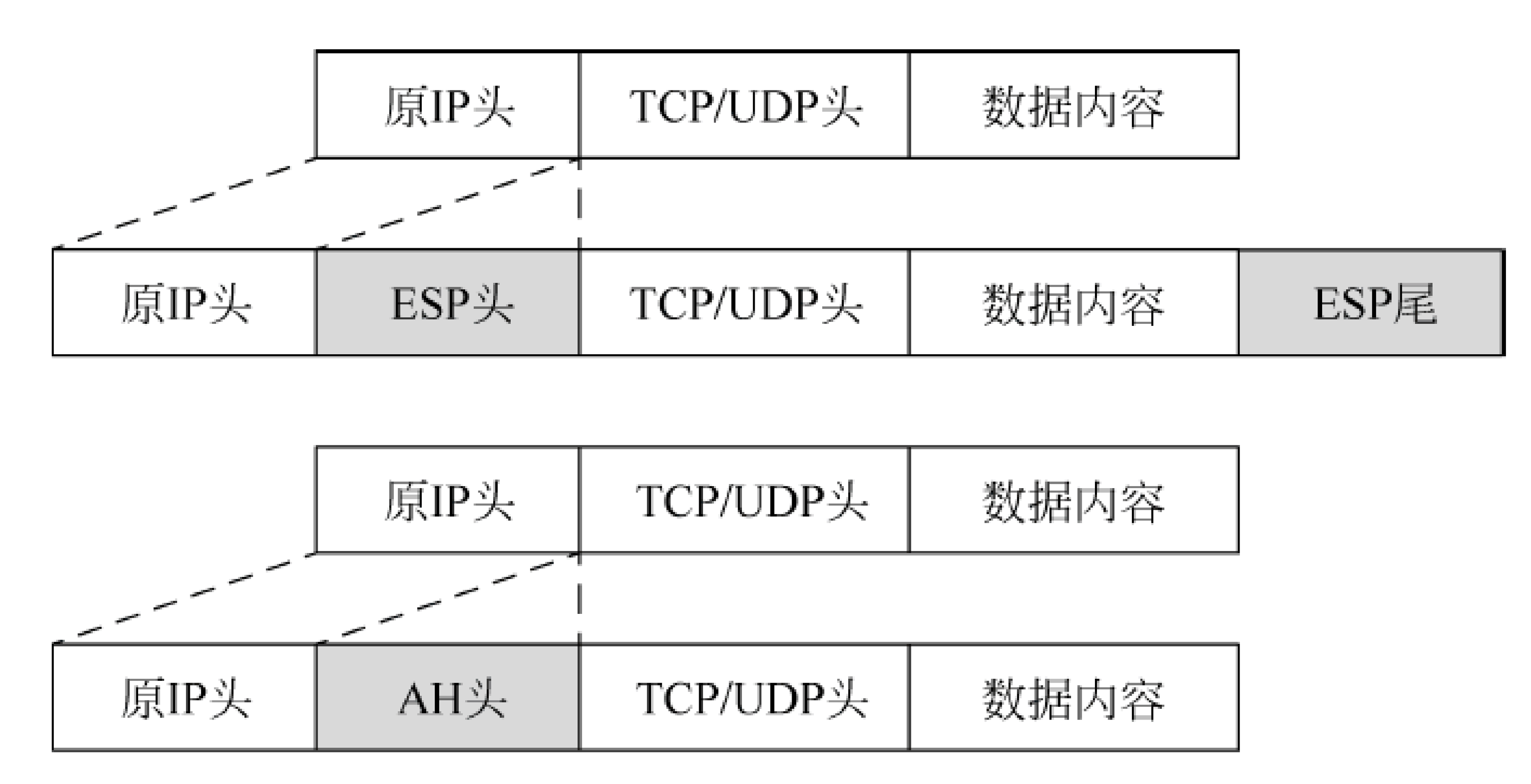


图 2-17　IPSec 的传输模式的 AH 和 ESP 封装示意图

2）隧道模式

采用隧道模式时，IPSec 对整个 IP 数据报进行加密或认证。此时，需要产生一个新的 IP 头，IPSec 头被放在新产生的 IP 头和原 IP 数据报之间，从而组成一个新的 IP 头。IPSec 隧道模式如图 2-18 所示。

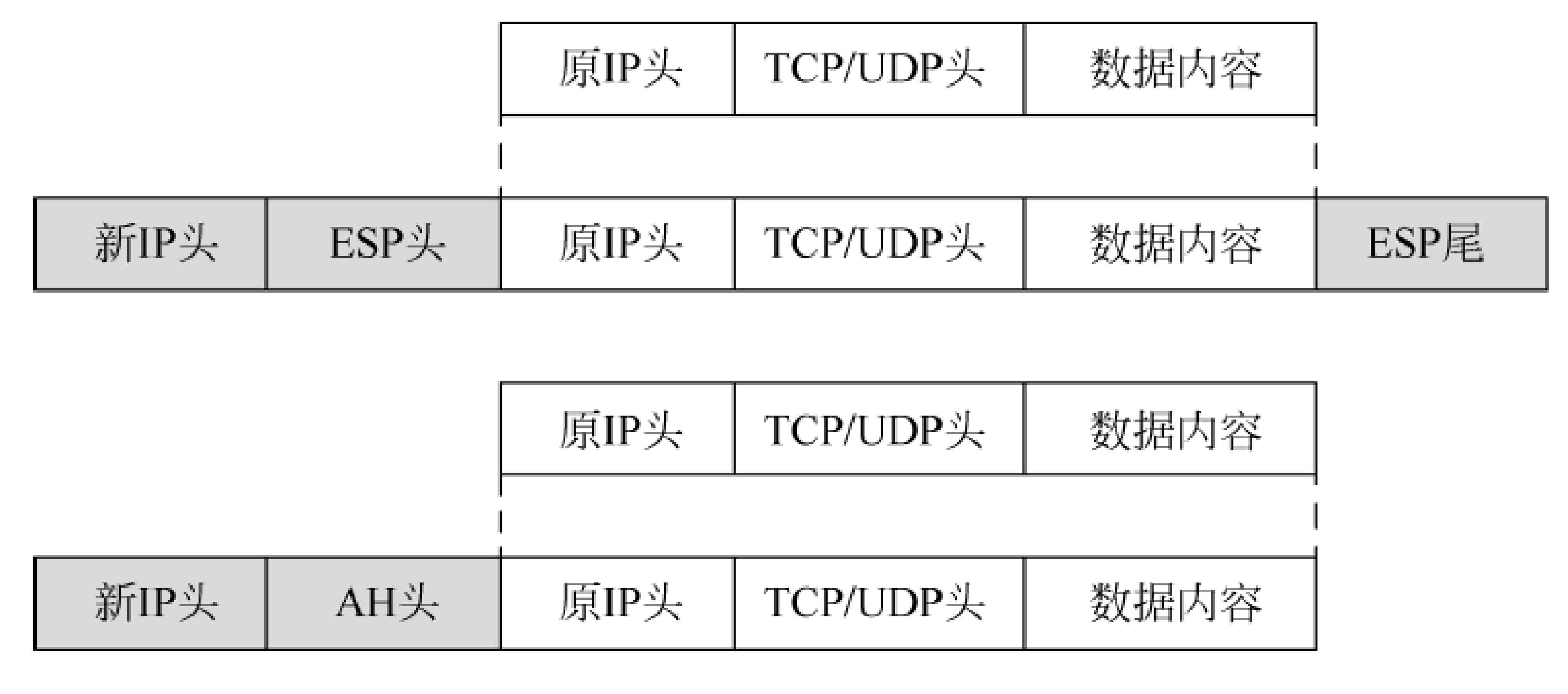


图 2-18　IPSec 隧道模式的 AH 封装示意图

2. IPSec 中的主要协议

IPSec 协议的主要功能为加密和认证。为了进行加密和认证，IPSec 还需要有密钥的管理和交换功能，以便为加密和认证提供所需要的密钥并对密钥的使用进行管理。以上三方面的工作分别由 AH、ESP 和 IKE 三个协议来实现。为了介绍这三个协议，需要先引入一个非常重要的术语——安全关联(Security Association，SA)。所谓安全关联，是指安全服务与它服务的载体之间的一个"连接"。AH 和 ESP 的实现都需要 SA 的支持，而 IKE 的主要功能就是建立和维护 SA。

如果要用 IPSec 建立一条安全的传输通路，通信双方需要事先协商好将要采用的安全策略，包括使用的加密算法、密钥、密钥的生存期等。当双方协商好使用的安全策略后，通常就说双方建立了一个 SA。给定了一个 SA，就确定了 IPSec 要执行的处理，如加密、认证等。

1) AH(Authentication Header，认证头)

RFC2402 的作者设计了 AH 协议来防御中间人攻击。RFC2402 对 AH 协议进行了极为详细的定义，将 AH 服务定义如下：

- 非连接的数据完整性校验
- 数据源点认证
- 可选的抗重放服务

AH 有两种实现方式：传输方式和隧道方式。当 AH 以传输方式实现时，它主要提供对高层协议的保护，因为高层的数据不进行加密。当 AH 以隧道方式实现时，协议被应用于通过隧道的 IP 数据报。

AH 只涉及认证，不涉及加密。AH 虽然在功能上与 ESP 有重复之处，但 AH 除了可以对 IP 的净荷进行认证外，还可以对 IP 头实施认证，而 ESP 的认证功能主要是面向 IP 的净荷。为了提供最基本的功能并保证互操作性，AH 必须提供对 HMAC SHA 和 HMAC MD-5(HMAC 是由杂凑函数 SHA 和 MD-5 构造的消息认证码)的支持。

AH 的长度是可变的，但必须是 32 位数据报长度的倍数。AH 域被细分为几个子域，其中包含为 IP 数据报提供密码保护所需的数据，如图 2-19 所示。

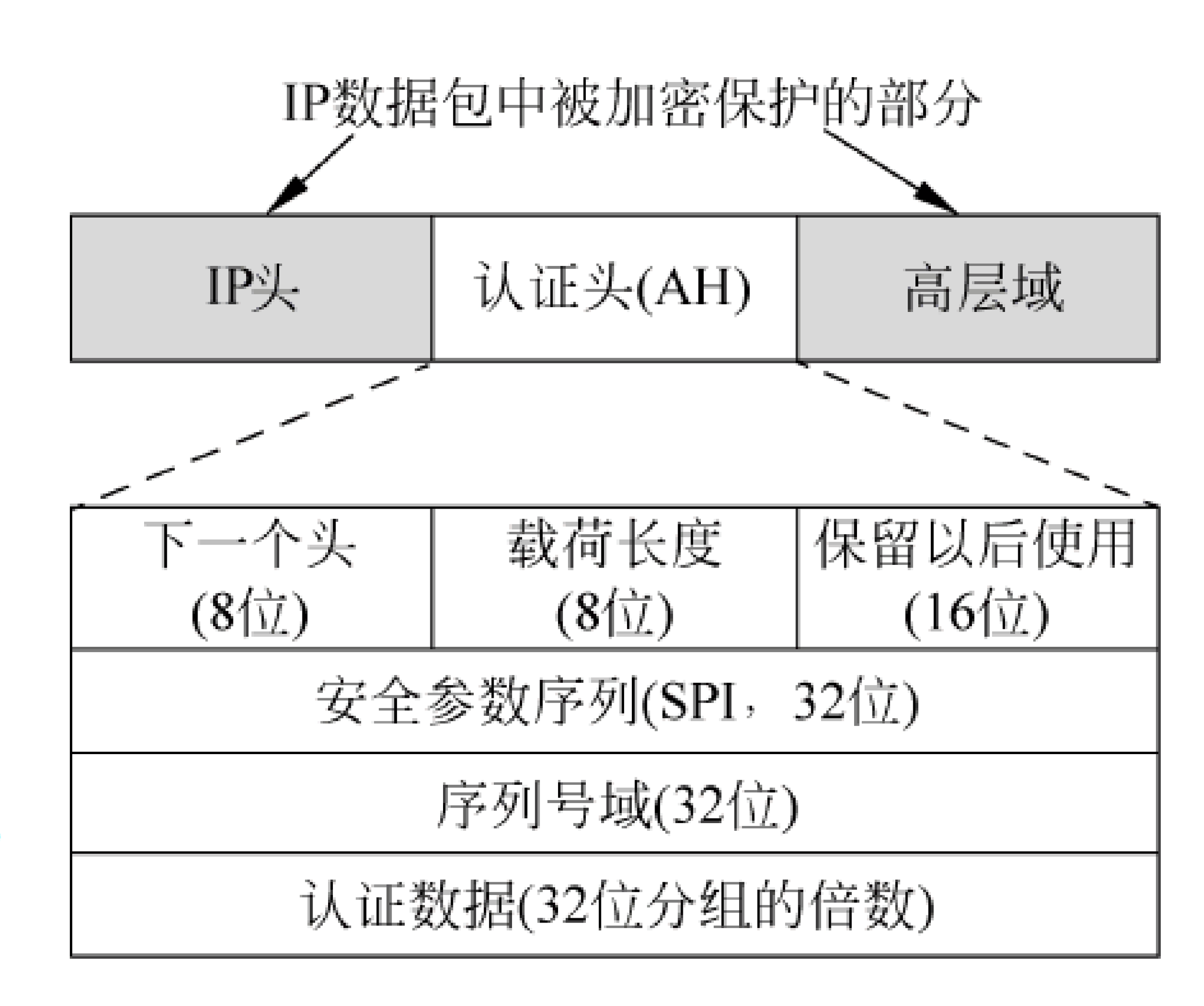


图 2-19　认证头的结构及其在 IP 数据报中的位置

数据源点认证是 IPSec 的强制性服务，它实际上提供了对源点身份数据的完整性保护。提供该保护所需的数据包含在 AH 的两个子域中，一个子域称为"安全参数索引"(Security Parameters Index，SPI)，包含长 32 位的某个任意值，用于唯一标识该 IP 数据报认证服务所采用的密码算法；另一个子域称为"认证数据"，包含消息发送方为接收方生成的认证数据，用于接收方进行数据完整性验证，因此这部分数据也被称为完整性校验值(Integrity Check Value，ICV)。该 IP 数据报的接收方能够使用密钥和 SPI 所标识的算法重新生成"认证数据"，然后将其与接收的"认证数

据”相比较，从而完成 ICV 校验。

AH 还有一个“序列号”子域，用来抵御 IP 数据报重放攻击。AH 的子域(包括“下一个头”“载荷长度”和“保留以后使用”)都没有安全方面的意义。

2) ESP

ESP(Encapsulating Security Payload)协议主要用于对 IP 数据报进行加密，此外也对认证提供某种程度的支持。ESP 独立于具体的加密算法，几乎可以支持各种对称密钥加密算法，如 DES、TripleDES 和 RC5 等。为保证各种 IPSec 实现之间的互操作性，目前要求 ESP 必须支持 56 位密钥长度的 DES 算法。ESP 的格式如图 2-20 所示。



图 2-20　ESP 格式

ESP 协议数据单元格式由三部分组成，除了头部、加密数据部分外，在实施认证时还包含一个可选尾部。头部有两个域：安全参数索引(SPI)和序列号(Sequence Number)域。使用 ESP 进行安全通信之前，通信双方需要先协商好一组将要采用的加密策略，包括所使用的加密算法、密钥及密钥的有效期等。SPI 用来标识发送方在处理 IP 数据报时使用了哪组加密策略，当接收方看到了这个标识后就知道如何处理收到的 IP 数据报。“序列号”用来区分使用同一组加密策略的不同数据包。被加密的数据部分除了包含原 IP 数据报的净荷外，还包括填充数据。填充数据是为了保证加密数据部分的长度满足分组加密算法的要求。这两部分数据在传输时要进行加密。“下一个头”(Next Header)用来标识净荷部分所使用的协议，它可能是传输层协议(TCP 或 UDP)，也可能是 IPSec 协议(ESP 或 AH)。

3) IKE

因特网密钥交换协议(Internet Key Exchange，IKE)用于动态建立安全关联(Security Associationg，SA)。由 RFC2409 描述的 IKE 属于一种混合型协议。IKE 使用两个阶段的 ISAKMP：在第一阶段，通信各方彼此建立一个已通过身份认证和安全保护的通道，即建立 IKE 安全关联；在第二阶段，利用这个既定的安全关联为 IPSec 建立安全通道。IKE 图解如图 2-21 所示。

IKE 定义了两个阶段：阶段 1 交换和阶段 2 交换。Oakley 定义了三种模式，分别对应 ISAKMP 的三个阶段：快速模式、主模式和野蛮模式。在阶段 1 交换，IKE 采用的是身份保护交换(“主模式”交换)，以及根据 ISAKMP 文档制定的“野蛮模式”交换；在阶段 2 交换，IKE 则采用了一种“快速模式”交换。

ISAKMP 通过 IKE 对以下几种密钥交换机制提供支持：

- 预共享密钥(PSK)

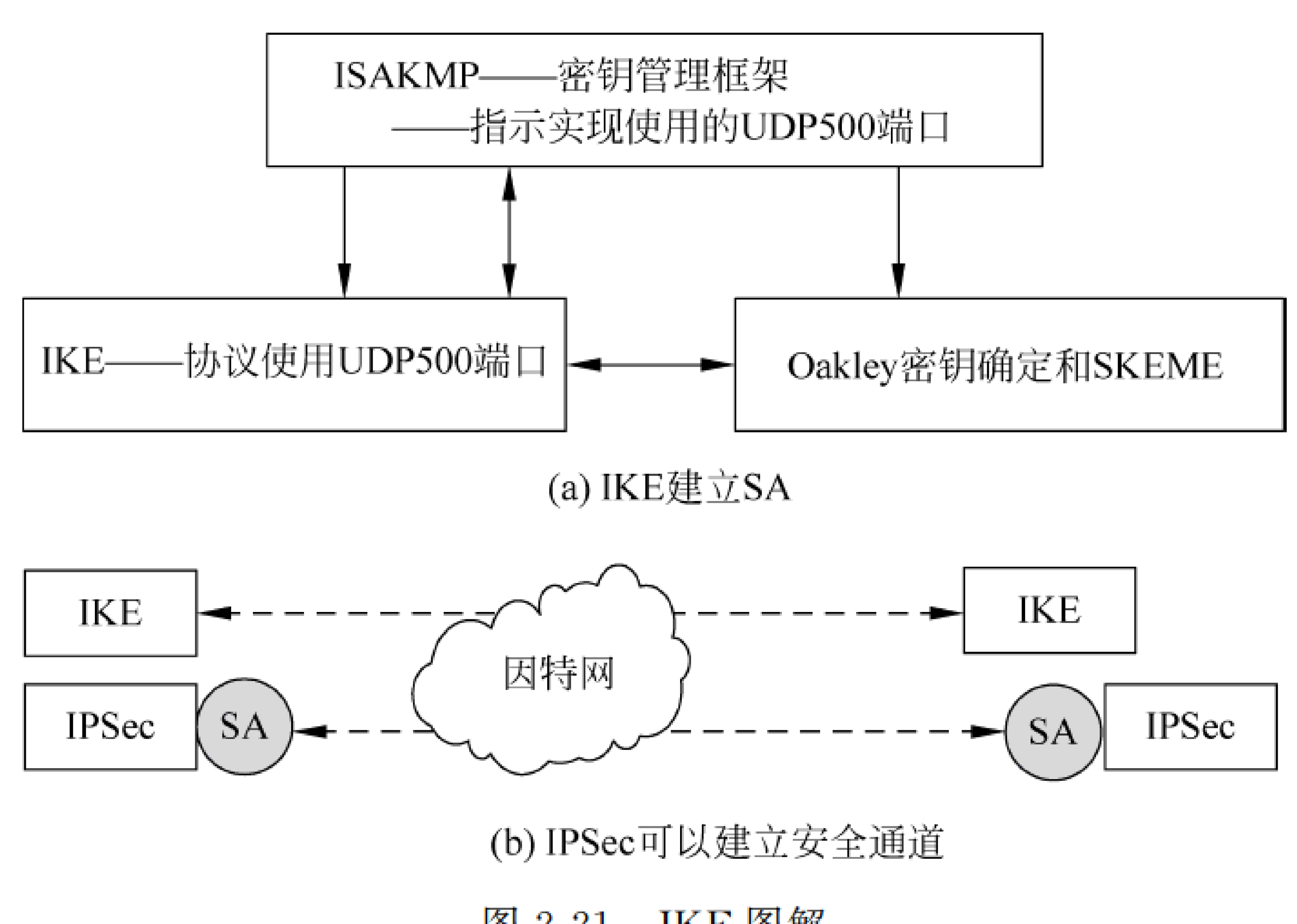


图 2-21　IKE 图解

- 公钥基础设施(PKI)
- IPSec 实体身份的第三方证书

预共享密钥(Preshared Secret Key,PSK)机制实质上是一种简单的口令方法。在 IPSec VPN 网关上预设常量字符串,通信双方据此共享秘密实现相互认证。总之,IKE 可以动态地建立安全关联和共享密钥。IKE 建立安全关联的实现极为复杂。一方面,它是 IPSec 协议实现的核心;另一方面,它也很可能成为整个系统的瓶颈。进一步优化 IKE 程序和密码算法是实现 IPSec 的核心问题之一。

3. 安全关联

IPSec 的中心概念之一是“安全关联”(Security Association,SA)。从本质上讲,IPSec 可被视为 AH+ESP。当两个网络节点在 IPSec 保护下通信时,它们必须协商一个 SA(用于认证)或两个 SA(分别用于认证和加密),并协商这两个节点间所共享的会话密钥以便它们能够执行加密操作。要在两个安全网关之间建立安全双工通信,需要为每个方向建立一个 SA。在 IPSec 当前的实现方案中,SA 管理机制只定义了单一特性的 SA。这意味着当前的 SA 只能建立点到点的通信。在未来,增强功能将会支持点到点及一点到多点的通信。

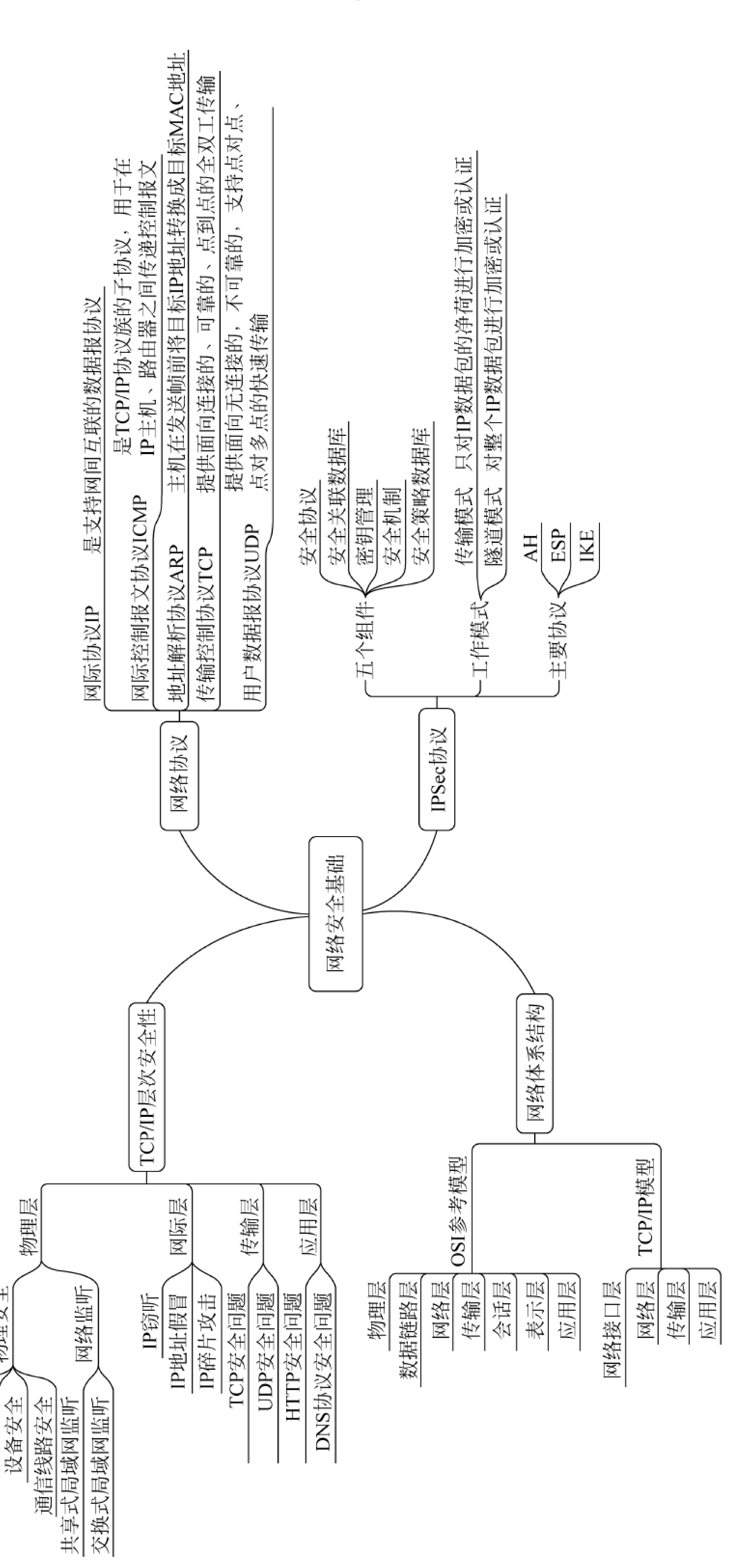
每个 SA 的标识由三部分组成:

- 安全性参数索引,即 SPI
- IP 目的地址
- 安全协议标识,即 AH 或 ESP

如前所述,SA 有两种模式,即传输模式和隧道模式。传输模式下的 SA 是两个主机间的安全关联;隧道模式下的 SA 只适用于 IP 隧道。如果在两个安全网关之间或一个安全网关和一个主机之间建立安全关联,那么此 SA 必须使用隧道模式。

当然,也可以将不同的 SA 组合起来使用,以提供多层次的安全性或封装能力。当对 SA 进行组合时,组合结果被称为一个 SA 束。此时,IPSec 在对传输数据进行处理时,也必须使用一系列的安全关联。

2.5 本章小结


网络安全基础
网络协议
网际协议IP
是支持网间互联的数据报协议
网际控制报文协议ICMP
是TCP/IP协议族的子协议，用于在IP主机、路由器之间传递控制报文
地址解析协议ARP
主机在发送帧前将目标IP地址转换成目标MAC地址
传输控制协议TCP
提供面向连接的、可靠的、点到点的全双工传输
用户数据报协议UDP
提供面向无连接的，不可靠的，支持点对点、点对多点的快速传输
IPSec协议
五个组件
安全协议
安全关联数据库
密钥管理
安全机制
安全策略数据库
工作模式
传输模式
只对IP数据包的净荷进行加密或认证
隧道模式
对整个IP数据包进行加密或认证
主要协议
AH
ESP
IKE
TCP/IP层次安全性
物理层
物理安全
环境安全
电源系统安全
设备安全
通信线路安全
网络监听
共享式局域网监听
交换式局域网监听
网际层
IP窃听
IP地址假冒
IP碎片攻击
传输层
TCP安全问题
UDP安全问题
应用层
HTTP安全问题
DNS协议安全问题
网络体系结构
OSI参考模型
物理层
数据链路层
网络层
传输层
会话层
表示层
应用层
TCP/IP模型
网络接口层
网络层
传输层
应用层

2.6 习　　题

一、填空题

1. OSI 参考模型包括物理层、(　　)、网络层、传输层、会话层、表示层和应用层。

2. (　　)是 OSI 参考模型的第 1 层。

3. 在 OSI 参考模型中控制网络层与物理层之间的通信的是(　　)。

4. TCP/IP 由 4 个层次组成，分别是(　　)、网络层、传输层和应用层。

5. (　　)又称为网际协议，是支持网间互联的数据报协议。

6. IPSec 的主要功能是实现加密、认证和密钥交换，这三个功能分别由(　　)、(　　)和(　　)三个协议来实现。

二、选择题

1. (　　)指令可以发现到达目标网络经过哪些路由器。

A. ping　　B. nslookup　　C. tracert　　D. ipconfig

2. 为了检测 Windows 系统是否有木马入侵，可以先通过(　　)命令来查看当前的活动连接端口。

A. ipconfig　　B. netstat -an　　C. tracert　　D. ping

3. ARP 欺骗的实质是(　　)。

A. 提供虚假的 MAC 和 IP 地址的组合　　B. 让其他计算机知道自己的存在

C. 窃取用户在网络中传输的数据　　D. 扰乱网络的正常运行

4. 在 Windows 操作系统中，对网关 IP 和 MAC 地址进行绑定的操作为(　　)。

A. ARP -a 192.168.1.1 00-0a-03-aa-5d-ff

B. ARP -d 192.168.1.1 00-0a-03-aa-5d-ff

C. ARP -s 192.168.1.1 00-0a-03-aa-5d-ff

D. ARP -g 192.168.1.1 00-0a-03-aa-5d-ff

5. 当用户通过域名访问某一合法网站时，打开的却是一个不健康的网站，发生该现象的原因可能是(　　)。

A. ARP 欺骗　　B. DHCP 欺骗

C. TCP SYN 攻击　　D. DNS 缓存中毒

6. 一个 IP 数据报由首部和数据两部分组成，首部的前一部分是固定长度，共(　　)字节，是所有 IP 数据报必须具有的。

A. 8　　B. 16　　C. 20　　D. 32

7. (　　)是 TCP/IP 协议族的子协议，用于在 IP 主机、路由器之间传递控制报文。

A. ICMP　　B. ARP　　C. IP　　D. TCP

8. (　　)命令可以删除 ARP 表中的所有内容。

A. arp -a　　B. arp -b　　C. arp -c　　D. arp -d

9. (　　)命令可以观察主机的 ARP 缓存表。

A. arp -a　　B. arp -b　　C. arp -c　　D. arp -d

10. (　　)可以提供面向无连接的,不可靠的,支持点对点、点对多点的快速传输。

A. TCP　　B. UDP　　C. IP　　D. ICMP

11. IPSec 协议和(　　)VPN 隧道协议处于同一层。

A. PPTP　　B. L2TP　　C. GRE　　D. 以上皆是

12. AH 协议中必须实现的验证算法是(　　)。

A. HMAC-MD5 和 HMAC-SHA1　　B. NULL

C. HMAC-RIPEMD-160　　D. 以上皆是

13. ESP 协议中不是必须实现的验证算法是(　　)。

A. HMAC-MD5　　B. HMAC-SHA1

C. NULL　　D. HMAC-RIPEMD-160

14. ESP 协议中必须实现的加密算法是(　　)。

A. 仅 DES-CBC　　B. 仅 NULL

C. DES-CBC 和 NULL　　D. 3DES-CBC

15. (　　)协议必须提供验证服务。

A. AH　　B. ESP　　C. GRE　　D. 以上皆是

16. IKE 协议由(　　)协议混合而成。

A. ISAKMP、Oakley、SKEME　　B. AH、ESP

C. L2TP、GRE　　D. 以上皆是

17. IPSec 在 OSI 参考模型的(　　)层提供安全性。

A. 应用　　B. 传输　　C. 网络　　D. 数据链路

18. IPSec 中的加密是由(　　)完成的。

A. AH　　B. TCP/IP　　C. IKE　　D. ESP

三、判断题

1. TCP/IP 体系有 7 个层次,ISO/OSI 体系有 4 个层次。
2. ARP 的作用是将物理地址转化为 IP 地址。
3. ARP 欺骗只会影响主机,而不会影响交换机和路由器等设备。
4. ICMP 报文是在 IP 数据报内部被传输的。
5. ICMP 的一个重要应用就是分组间探测 ping,用来测试两个主机之间的连通性。

四、简答题

1. OSI 参考模型是什么?TCP/IP 模型是什么?(由低到高)
2. TCP 与 UDP 的区别是什么?
3. IPSec 有哪两种工作模式?两种工作模式有什么不同?

第 3 章　网络攻击技术

【本章学习目标】

- 了解黑客概念和黑客分类
- 掌握网络攻击的定义
- 理解黑客攻击步骤
- 掌握代理跳板的原理和方法
- 了解信息搜集的种类
- 掌握网络扫描的步骤
- 掌握操作系统探测技术原理
- 了解各种网络攻击方法
- 掌握 DDoS 攻击原理与防御方法

3.1　黑　　客

3.1.1　黑客概念

黑客是 Hacker 的音译,源于动词 Hack,其引申意义是“干了一件非常漂亮的事”。在这里我们所说的黑客是指那些精于某方面技术的人。对于计算机而言,黑客就是精通网络、系统、外设以及软硬件技术的人。

黑客最早出现于 20 世纪 50 年代,最早的计算机于 1946 年在宾夕法尼亚大学诞生,而最早的黑客出现于麻省理工学院。最初的黑客是一些高级技术人员,他们热衷于挑战、崇尚自由并主张信息的共享。但到了今天,黑客一词已被泛指那些专门利用计算机搞破坏或恶作剧的家伙,对这些人的正确叫法是 Cracker,有人也翻译成骇客或是入侵者。

3.1.2　黑客分类

第一种分类是将黑客分为破坏者、红客和间谍,如图 3-1 所示。

(1) 破坏者:以破坏为主的黑客。

(2) 红客:红客一词比较容易理解,有很强的政治性,红客的行为旨在抗击外来网络入侵,维护国内网络安全,有很强的爱国色彩。

(3) 间谍:专门为了利益而去做一些破坏或窃取一些信息。

第二种分类是将黑客分为白帽子、黑帽子和灰帽子。

(1) 白帽子:是创新者。研究漏洞,追求先进技术并与大家共享的黑客称为“白帽子”。

（2）黑帽子：是破坏者。以破坏和入侵为目的的黑客称为“黑帽子”。

（3）灰帽子：是破解者。介于以上二者之间的叫作“灰帽子”，这是一个追求网上信息公开的群体，他们不破坏，但要进入别人的网站读取信息。

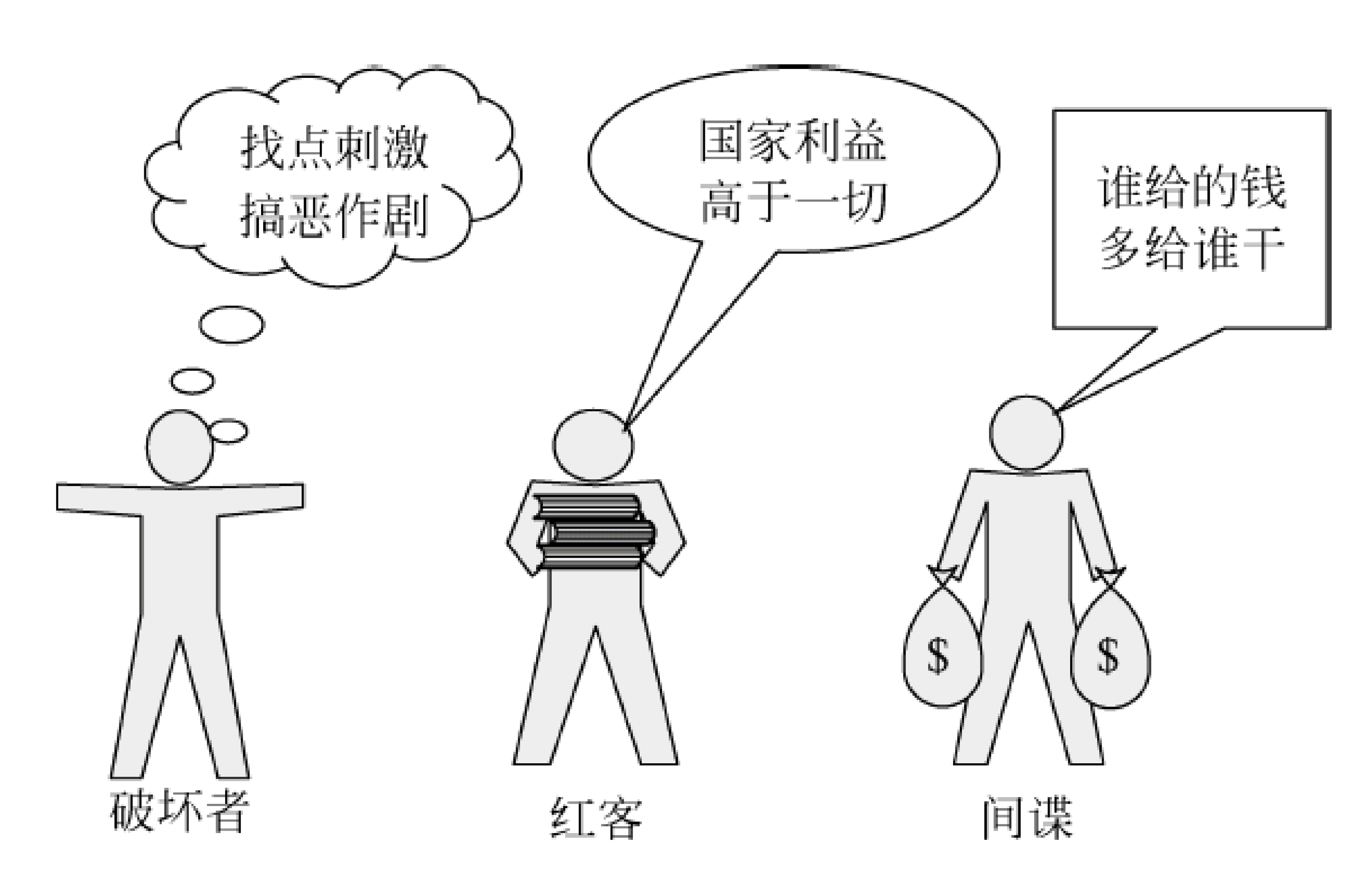


图 3-1　黑客分类

3.1.3　黑客行为发展趋势

黑客行为有以下 7 个方面的发展趋势。

（1）手段高明化：综合各种流行的攻击方法，技巧性更强，更容易得手。例如，guest 账户显示为禁用状态，但能用其登录而且拥有管理员权限，这就用到了留后门的方法，如果管理员不知道这种黑客手段，就很难发现已被入侵。

（2）活动频繁化：黑客行为将越来越频繁，查看一台刚刚启动几分钟的服务器，就可在它的各种日志中发现黑客攻击的痕迹。

（3）动机复杂化：黑客行为的动机也更加复杂，有政治目的、个人目的和商业目的等。

（4）黑客年轻化：由于互联网的普及，形成全球一体化，甚至很多偏远地区也可以从网络上接触到世界各地的信息资源，所以越来越多对黑客攻击感兴趣的中学生也已经踏足到这个领域。

（5）破坏力扩大化：因互联网的普及，电子商务也在蓬勃发展，全社会对互联网的依赖性日益增强，黑客的破坏力也日益扩大化。仅在美国，黑客每年造成的经济损失就超过 100 亿美元。

（6）黑客技术普及化：黑客组织的形成和黑客傻瓜式工具的大量出现导致的一个直接后果就是黑客技术的普及。在互联网上，传授黑客技术的站点比比皆是，这些黑客站点提供黑客工具，公布系统漏洞，公开传授黑客技术，进行黑客教学，甚至还提供网上论坛、网上聊天工具以相互交流黑客技术经验，协调黑客行动。黑客事件的剧增，黑客组织规模的扩大，黑客站点的大量涌现，也说明了黑客技术开始普及，甚至很多十几岁的年轻人也有了自己的黑客站点，从很多论坛上可以看到学习探讨黑客技术的人也越来越多。

（7）黑客组织化：因为利益的驱使，黑客开始由原来的独立个体变成有组织的黑客群体，在黑客组织内部，成员之间相互交流技术经验，共同采取黑客行动，行动的成功率增高，影响力也更大。

3.2　网络攻击概述

3.2.1　网络攻击定义

网络攻击是对网络系统的机密性、完整性、可用性等产生危害的行为。实际上，网络攻击是黑客利用被攻击方网络系统自身存在的漏洞，通过使用网络命令和专用软件侵入其网络系统实施的攻击。

3.2.2　网络攻击分类

X.800 和 RFC 2828 对网络攻击进行了分类。它们把攻击分为两类：被动攻击和主动攻击。被动攻击试图获得或利用系统的信息，但不会对系统的资源造成破坏。而主动攻击则不同，它试图破坏系统的资源，影响系统的正常工作。

1. 被动攻击

被动攻击的特性是对所传输的信息进行窃听和监测，攻击者的目标是获得线路上所传输的信息。窃听攻击和流量分析就是两种被动攻击的例子。

(1) 窃听攻击。如图 3-2 所示，电子邮件和传输的文件中都可能包含敏感或秘密信息，攻击者通过窃听，可以截获这些敏感或秘密信息，网络管理人员的工作就是阻止攻击者获得这些信息。

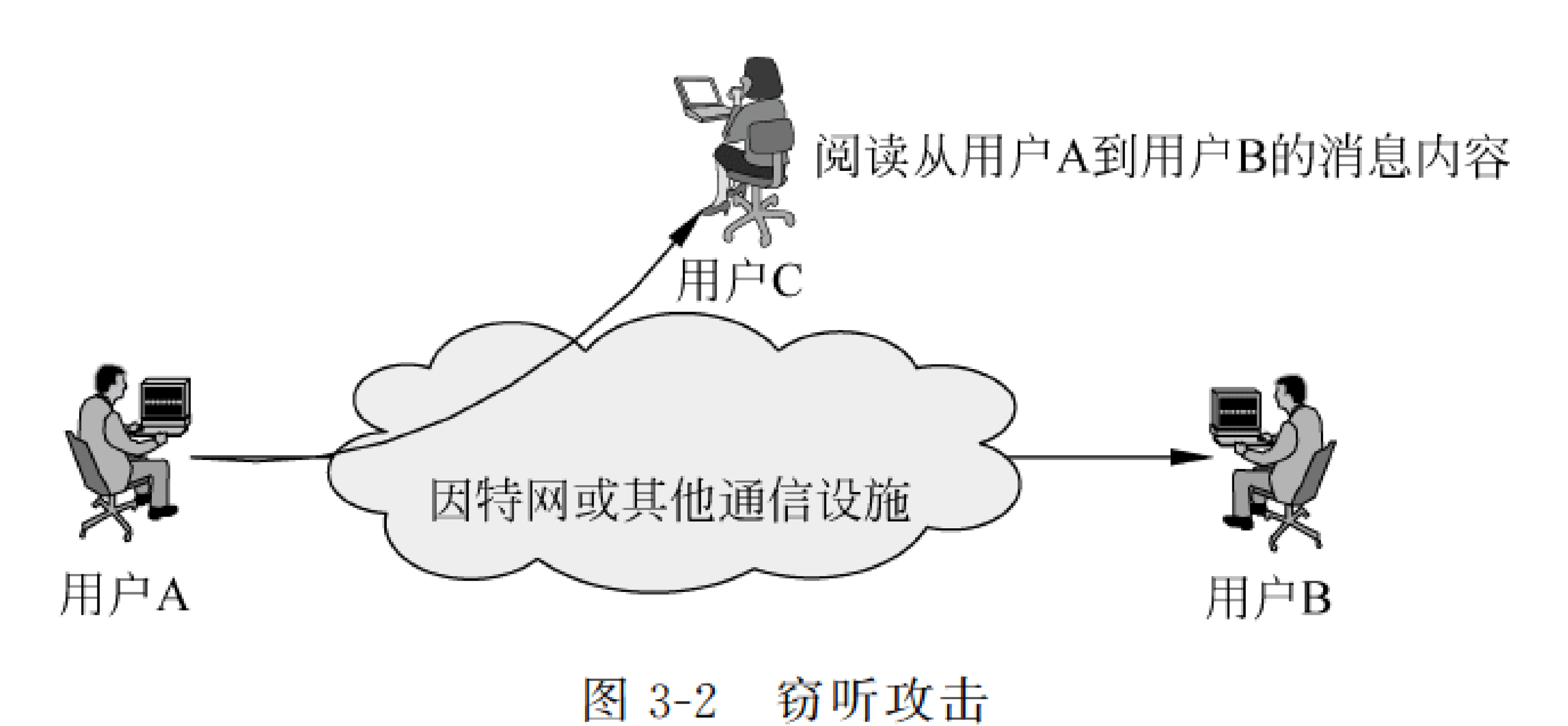


图 3-2　窃听攻击

(2) 流量分析。如图 3-3 所示，假设已经采取了某种措施来隐藏消息内容或其他信息的流量，使攻击者即使捕获了消息也不能从中发现有价值的信息。加密是隐藏消息的常用方法，即使对消息进行了合理的加密保护，攻击者仍然可以通过流量分析获得这些消息的模式。攻击者可以通过确定主机的身份及其所处的位置，观察传输消息的频率和长度，然后根据所获得的信息推断本次通信的性质。

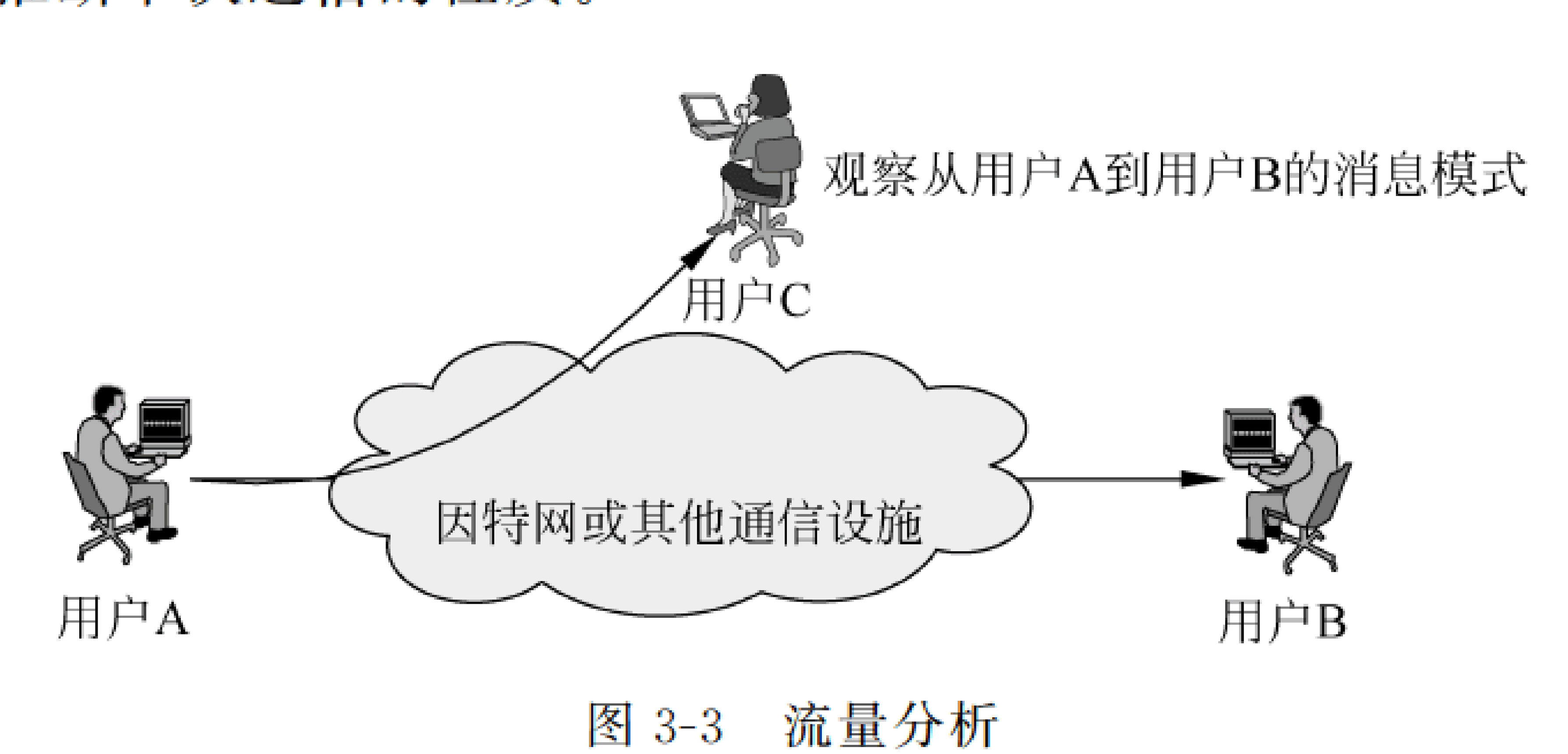


图 3-3　流量分析

由于被动攻击不涉及对数据的更改,所以很难被察觉。通过采用加密措施,完全有可能阻止这种攻击。因此,处理被动攻击的重点是预防,而不是检测。

2. 主动攻击

主动攻击是指恶意篡改数据流或伪造数据流等攻击行为,它一般分为以下 4 类。

(1) 伪装攻击。伪装攻击是指某个实体假装成其他实体,对目标发起攻击,如图 3-4 所示。例如,攻击者捕获认证信息,然后将其重发,这样攻击者就有可能获得其他实体所拥有的访问权限。



图 3-4 伪装攻击

(2) 重放攻击。重放攻击是指攻击者为了达到某种目的,将获得的消息再次发送,以在非授权的情况下进行传输,如图 3-5 所示。

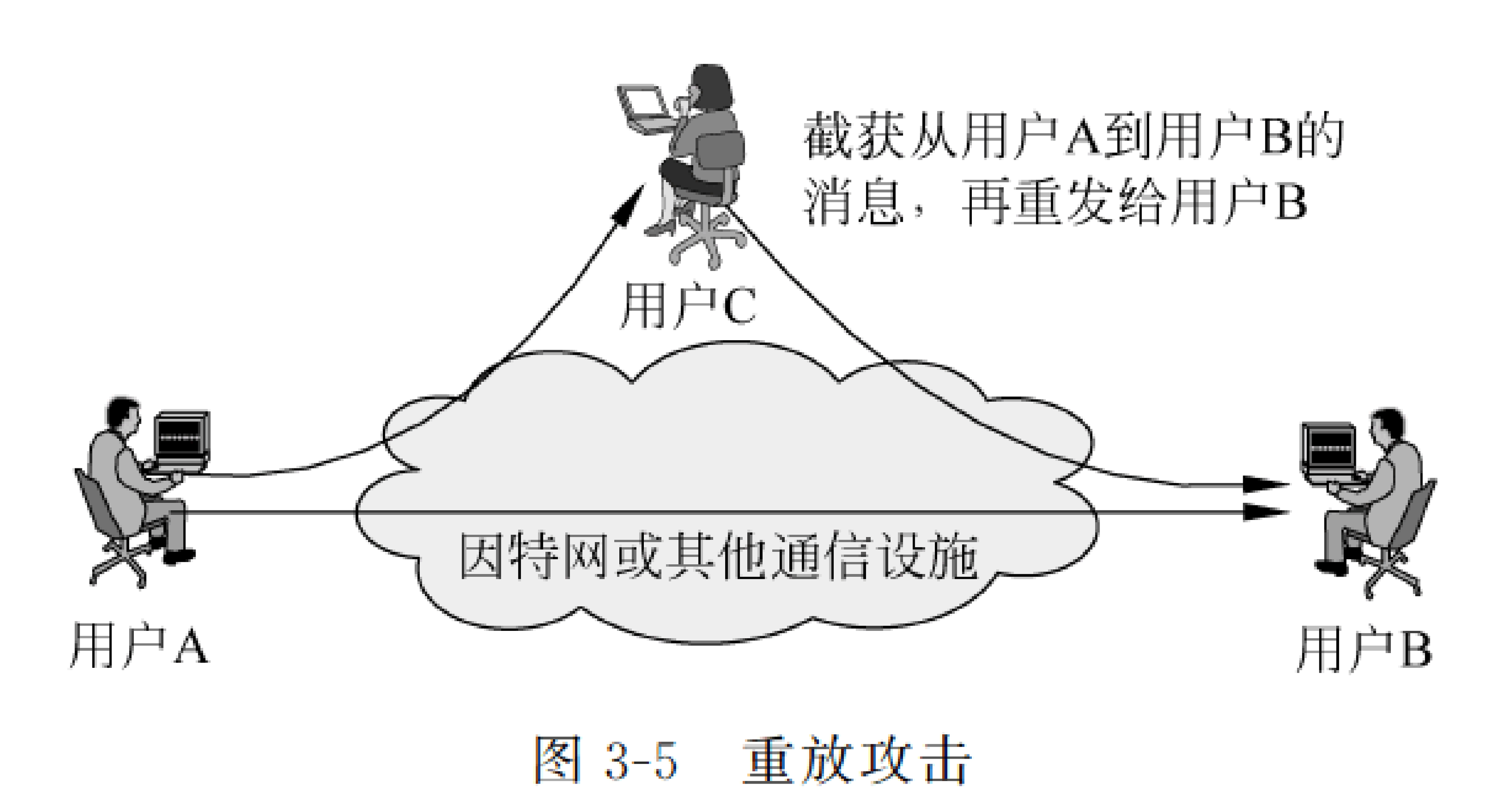


图 3-5 重放攻击

(3) 消息篡改。消息篡改是指攻击者对所获得的合法消息中的一部分进行修改或延迟消息的传输,以达到其非授权的目的,如图 3-6 所示。

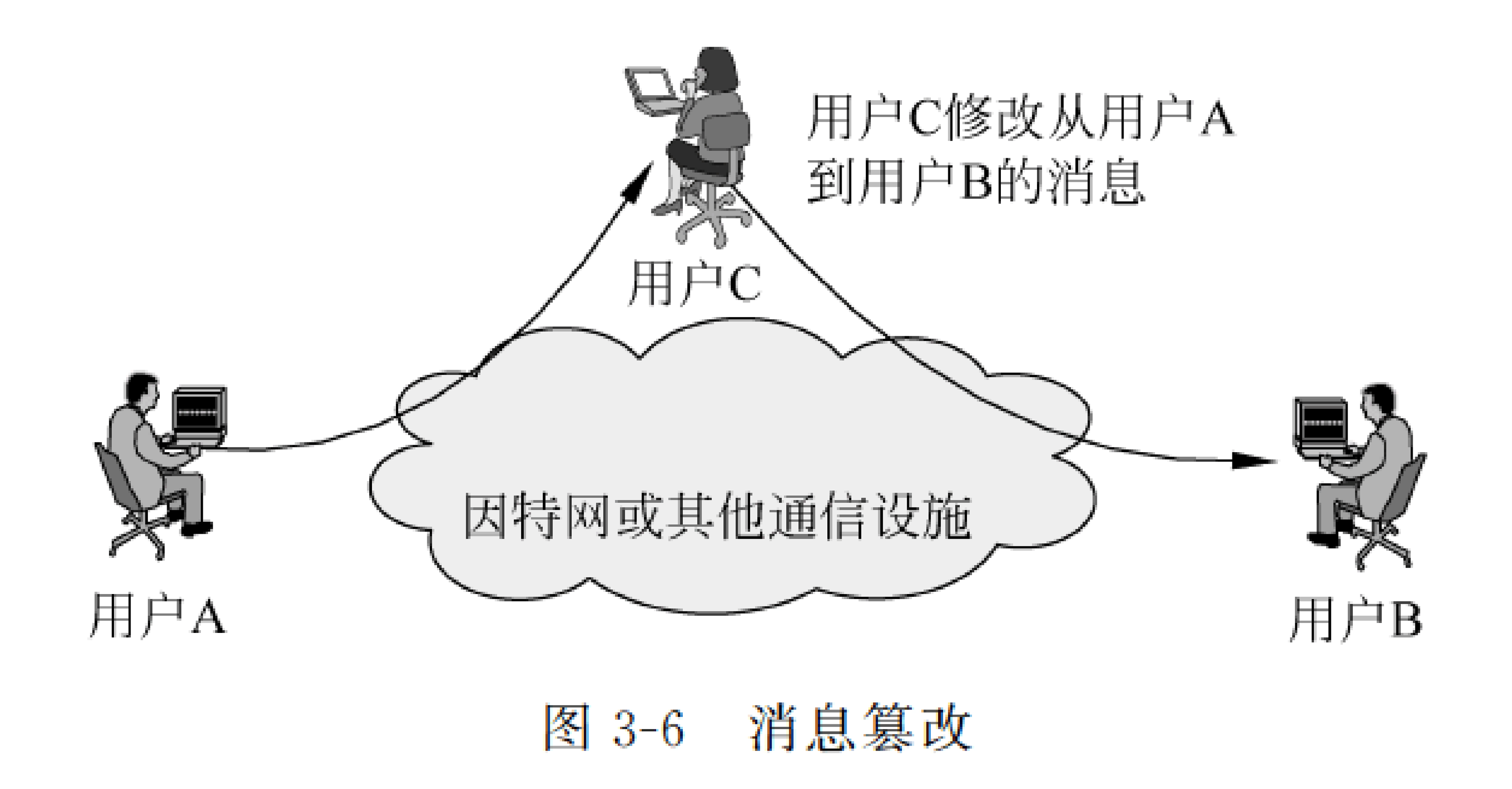


图 3-6 消息篡改

(4) 拒绝服务攻击。拒绝服务攻击是指阻止或禁止人们正常使用网络服务或管理通信设备,如图 3-7 所示。



图 3-7 拒绝服务攻击

主动攻击与被动攻击相反，被动攻击虽然难以检测，但采取某些安全防护措施就可以有效阻止；主动攻击虽然易于检测，但却难以阻止。所以对付主动攻击的重点应当放在如何检测并发现它们上，并采取相应的应急响应措施，使系统从故障状态恢复到正常运行。

3.2.3 网络攻击五部曲

一次成功的入侵攻击，可以归纳成基本的 5 个步骤，即人们常说的“网络攻击五部曲”，如图 3-8 所示，具体步骤和顺序可根据攻击时的实际情况随时进行调整。

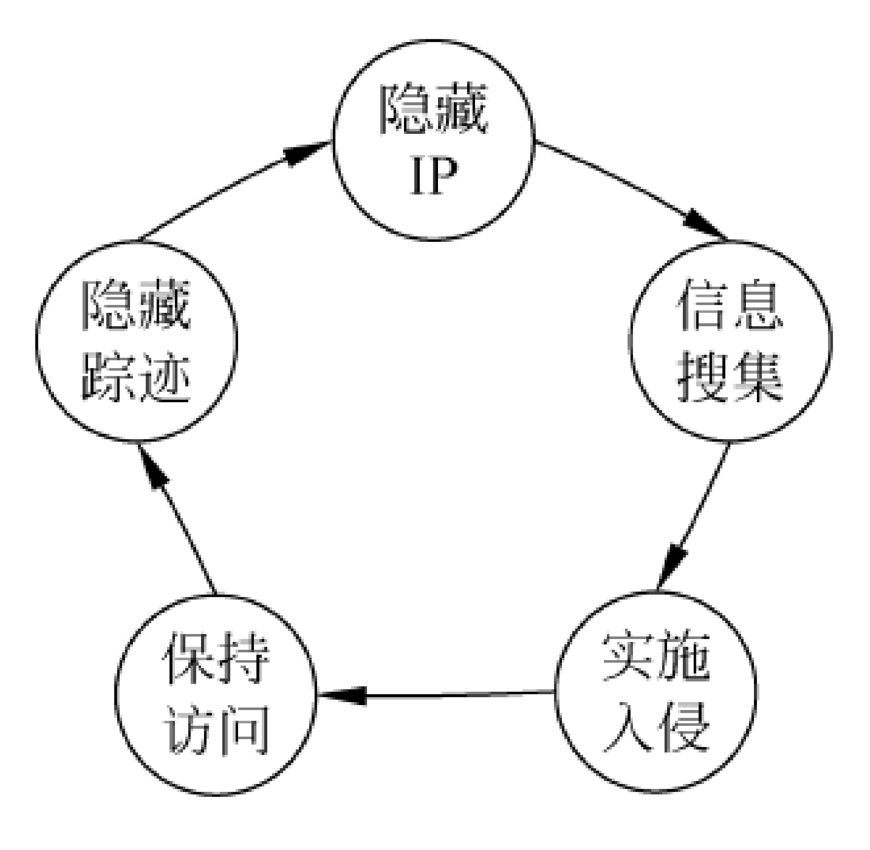


图 3-8 网络攻击五部曲

1. 隐藏 IP

当入侵者找到远程主机/服务器的系统缺陷后，会对其进行试探性的入侵，此时，入侵者将要面对的可能是缺乏经验的个人计算机用户，也可能是网络安全专家，或是对方布下的一个网络陷阱。所以，对于有经验的入侵者，他们会在入侵时步步小心，使用各种方法来隐藏自己，尽量不去直接与目标接触，以免暴露给远程主机/服务器。

2. 信息搜集

信息搜集俗称踩点，就是通过各种途径对所要攻击的目标进行多方面的了解。

3. 实施入侵

入侵者得到管理员权限，连接到远程计算机，对其进行控制，达到自己攻击的目的。

4. 保持访问

入侵者为了保持长期对胜利果实的访问权，在已经攻破的计算机上种植一些供自己访问的后门。

5. 隐藏踪迹

一次成功的入侵，一般会在对方的计算机上存储相关的登录日志，这样就容易被管理员发现。在入侵完毕后需要清除登录日志及其他相关的日志。

3.3 隐藏 IP

任何攻击者都不希望自己的攻击行为被暴露，所以在实施攻击之前的首要任务是隐藏自己的 IP 地址。

通常有以下两种方式可以实现隐藏 IP 地址的效果。

(1) IP 欺骗。利用别人的主机(俗称"肉鸡")进行攻击,也就是说黑客首先登录到一个第三方的主机,然后再对目标进行攻击,这样一旦被发现,被攻击者也只能得到那台"肉鸡"的 IP。

(2) 网络代理跳板。做多级跳板代理,这样在被攻击者的主机上留下的将是代理跳板主机的 IP 地址。

3.3.1 IP 欺骗

1. IP 欺骗概述

所谓 IP 欺骗,就是伪造某台主机的 IP 地址的技术,其实质是让一台主机扮演另一台主机,以达到隐藏自己的目的。IP 欺骗通常要通过编写程序来实现,IP 欺骗者通过使用 RAW Socket 编程,发送带有假冒的源 IP 地址的 IP 数据报,来达到自己的目的。另外,网络上也有大量可以发送伪造的 IP 地址的工具,使用这些工具可以任意指定源 IP 地址,以免留下自己的痕迹。

IP 是网络层的一个面向无连接的协议,IP 数据报的主要内容由源 IP 地址、目的 IP 地址和所传数据构成,IP 的任务就是根据每个数据报文的目的地址,路由完成报文从源地址到目的地址的传送。至于报文在传送过程中是否丢失或出现差错,IP 不会考虑,对 IP 来讲,源设备与目的设备没有什么关系,它们是相互独立的。IP 包只是根据数据报文中的目的地址发送,因此借助高层协议的应用程序来伪造 IP 地址是比较容易实现的。

在 IP 欺骗的状态下,三次握手的情况如下。

第一步:黑客假冒主机 A 的 IP 向服务方主机 B 发送 SYN,告诉主机 B 是它所信任的主机 A 想发起一次 TCP 连接,序列号为数值 X,这一步实现比较简单,黑客将 IP 包的源地址伪造成主机 A 的 IP 地址即可。

要注意的是,在攻击的整个过程中,必须使主机 A 与网络的正常连接中断。因为 SYN 请求中 IP 包源地址是主机 A 的,当主机 B 收到 SYN 请求时,将根据 IP 包中源地址反馈 ACK SYN 给主机 A,但事实上主机 A 并未向主机 B 发送 SYN 请求,所以主机 A 收到后会认为这是一次错误的连接,从而向主机 B 回送 RST,中断连接。为了解决这个问题,在整个攻击过程中需要设法停止主机 A 的网络功能,使之拒绝服务即可。

第二步:服务方主机 B 产生 SYN ACK 响应,并向请求方主机 A(注意:是主机 A,不是黑客,因为主机 B 收到的 IP 包的源地址是主机 A)发送 ACK,ACK 的值为 X+1,表示数据成功接收到,且告知下一次接收到字节的 SEQ 是 X+1,同时,主机 B 向请求方主机 A 发送自己的 SEQ,注意这个数值对黑客是不可见的。

第三步:黑客再次向服务方发送 ACK,表示接收到服务方的回应。虽然实际上它并没有收到服务方主机 B 的 SYN ACK 响应,这次它的 SEQ 值为 X+1,同时它必须猜出 ACK 的值,并加 1 后回馈给主机 B。

如果黑客能成功地猜出主机 B 的 ACK 的值,那么 TCP 的三次握手就宣告成功,主机 B 会将黑客看作主机 A。黑客主机这种连接是"盲人"式的,黑客永远不会收到来自主机 B 的包,因为这些反馈包都被路由到主机 A 那里了。

由三次握手我们可以看出,IP 欺骗的关键在于猜出在第二步服务方所回应的 SEQ 值,有了这个值,TCP 连接方可成功地建立。在早期,这是个令人头疼的问题,但随着 IP 欺骗攻击手段的研究日益深入,一些专用的算法得到应用,并产生了一些专用的 C 程序,如

SEQ-Scan 等，当黑客使用这些 C 程序时，一切问题均可迎刃而解。

2. IP 欺骗的防备

1）防备网络外部的欺骗

对于来自网络外部的欺骗，阻止这种攻击的方法是很简单的。在局部网络的对外路由器上加一个限制条件，设置不允许声称来自于内部网络的外来包通过即可。尽管路由器可以通过分析测试源地址来解决 IP 欺骗中的一般问题，但是如果网络还存在外部的可信任主机，那么路由器就无法防止别人冒充这些主机而进行 IP 欺骗。

2）监视网络

通过对信息包的监控来检查 IP 欺骗这种攻击将是非常有效的方法。使用 NETLOG 等信息包检查工具对信息的源地址和目的地址进行检查，如果发现了信息包来自两个以上不同的地址，即说明系统有可能受到 IP 欺骗，防火墙外面正有黑客试图入侵系统。

3）安装过滤路由器

检测和保护站点免受 IP 欺骗的最好方法是安装一个过滤路由器，来限制对外部接口的访问，禁止带有内部网络资源地址包的通过。当然也应禁止（过滤）带有不同内部资源地址的内部包通过路由器到外部网络上去，这样即可防止内部用户对别的站点进行 IP 欺骗。

3.3.2 网络代理跳板

当从本地入侵其他主机时，自己的 IP 会暴露给对方，通过将某一台主机设置为代理，通过该主机再入侵其他主机，就会留下代理的 IP 地址，这样可以有效地保护自己的安全。这种二级代理的基本结构如图 3-9 所示。

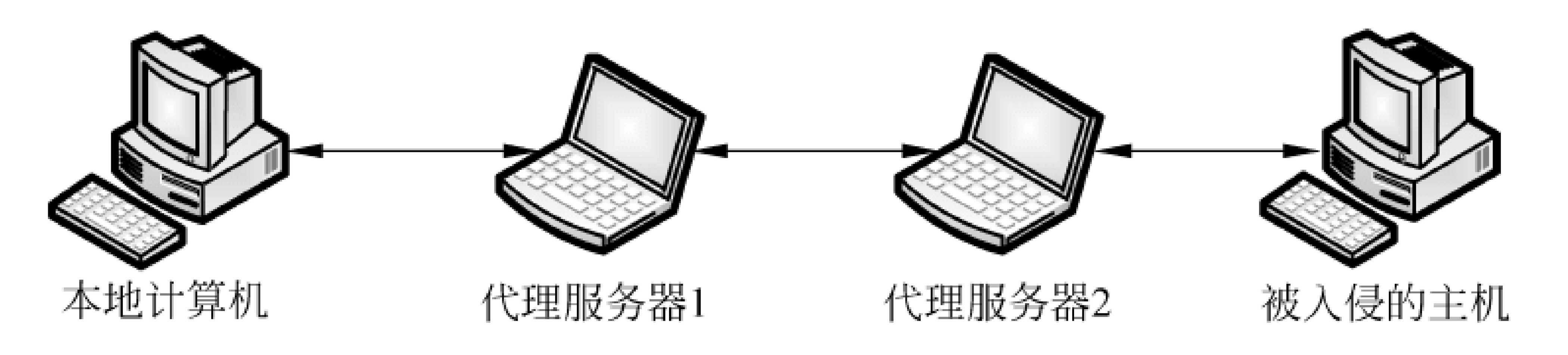


图 3-9　二级代理的基本结构

本地计算机通过两级代理入侵某一台主机，这样在被入侵的主机上，不会留下自己的信息。可以选择更多的代理级别，但是考虑到网络带宽的问题，一般选择两级或三级代理比较合适。能否被选择做代理主机有一个首要条件，即必须先安装相关的代理软件，一般是将已经入侵的主机作为代理服务器。

3.4 网络扫描

3.4.1 网络扫描概述

在攻击者对特定的网络资源进行攻击之前，他们需要了解将要攻击的环境，这需要搜集、汇总各种和目标系统相关的信息，包括主机数目、类型、操作系统等。

网络扫描技术是一种重要的网络安全技术。扫描本身不算一种攻击行为，但是它常常可以作为攻击发起前的准备工作。扫描器能够自动检测远程或本地主机的安全性弱点，发现远程服务器各种 TCP 端口的分配、提供的服务及相应的软件版本，记录目标给予的回答，

搜集关于目标主机的各种有用信息。扫描器可以帮助发现目标主机存在的一些问题，而这些问题可能恰恰就是黑客攻击的关键点。

反之，网络管理员同样可以利用安全扫描技术与防火墙、入侵检测系统互相配合，有效提高网络的安全性。通过对网络的扫描，网络管理员可以了解网络的安全配置和运行的应用服务，及时发现安全漏洞，客观评价网络风险等级。网络管理员可以根据扫描的结果更正网络安全漏洞和系统中的错误配置，在黑客攻击前进行防范。如果说防火墙和网络监控系统是被动的防御手段，那么安全扫描就是一种主动的防范措施，可以有效避免黑客攻击行为，做到防患于未然。

3.4.2　网络扫描步骤

一次完整的网络扫描分为以下三个阶段。

(1) 第一阶段：发现目标主机或网络。

(2) 第二阶段：发现目标后进一步搜集目标信息，包括操作系统类型、运行的服务及服务软件的版本等。如果目标是一个网络，还可以进一步发现该网络的拓扑结构、路由设备以及各主机的信息。

(3) 第三阶段：根据搜集到的信息判断或者进一步测试系统是否存在安全漏洞。

网络扫描技术包括：Ping 扫射、操作系统探测、端口扫描及漏洞扫描等。这些技术在网络扫描的三个阶段中各有体现。

1. Ping 扫射技术

Ping 扫射技术用于网络安全扫描的第一阶段，可以帮助我们识别系统是否处于活动状态。在公司里，一天中的不同时间有不同的主机在活动，攻击者想知道哪些主机是活动的，哪些不是，他们一般在白天寻找活动的主机，然后在深夜再次查找，这样就能区分工作站和服务器。

2. 操作系统探测技术

操作系统探测技术用于网络安全扫描的第二阶段，攻击者已知哪些主机是活动的，下一步要识别每台主机运行哪种操作系统。因为对于不同类型的操作系统，其上的系统漏洞有很大区别，甚至同一种操作系统的不同版本的系统漏洞也是不一样的，所以攻击的方法也完全不同。

操作系统探测技术的原理是不同的操作系统在网络底层协议的各种实现细节上略有不同，扫描程序通过向远程主机发送不平常的或者没有意义的数据包来进行探测，因为这些数据包 RFC 在互联网标准中没有列出，每个操作系统对它们的处理方法不同，扫描程序通过解析输出，能够弄清自己正在访问的设备运行的是何种操作系统。

3. 端口扫描技术

端口扫描技术同样用于网络安全扫描的第二阶段，端口扫描是通过与目标系统的 TCP/IP 端口连接，查看该系统处于监听或运行状态的服务。

端口扫描也是一种获取主机信息的有效方法。在 UNIX/Linux 系统中，任何用户均可使用端口扫描程序而不需要 root 权限。从扫描的端口数目和端口号可以判断出目标主机运行的操作系统，通过收集扫描的信息，能够轻松地掌握局域网络的构造。表 3-1 所示为一些常用端口号和对应服务的对照表，不过应该认识到，这种对应仅仅是约定，并没有严格的规范进行约束，特别是对于高于 1024 的端口。

1）端口分类

（1）熟知端口号：由因特网指派名字和号码，公司负责分配给一些常用的应用层程序固定使用，其数值一般为 0～1023。

（2）一般端口号：用来随时分配给请求通信的客户进程。

表 3-1　常用服务端口对照表

服　务	端　口	服　务	端　口
socks	1080/tcp	wins	1512/tcp
socks	1080/udp	nfs	2049/tcp 2049/udp
mysql	3306/tcp 3306/udp	gopher	70/tcp 70/udp
netstat	15/tcp	finger	79/tcp 79/udp
linuxconf	98/tcp	http	80/tcp 80/udp
rndc	953/tcp 953/udp	pop3	110/tcp 110/udp
squid	3128/tcp	imap	143/tcp 143/udp
ftp	21/tcp 21/udp	ldap	389/tcp 389/udp
ssh	22/tcp 22/udp	rtsp	544/udp
telnet	23/tcp 23/udp	shell	514/tcp
smtp	25/tcp 25/udp	syslog	514/udp
nameserver	42/tcp 42/udp	uucp	540/tcp

2）端口扫描原理

入侵者如果想要探测目标计算机开放了哪些端口，提供了哪些服务，就需要先与目标端口建立 TCP 连接，这也就是扫描的出发点。尝试与目标主机的某些端口建立连接，如果目标主机该端口有回复（即三次握手中的第二次），则说明该端口开放，即为“活动端口”。

3）端口扫描原理分类

端口扫描原理分为三类，如图 3-10 所示，分别为全连接扫描、半连接扫描以及无连接扫描。

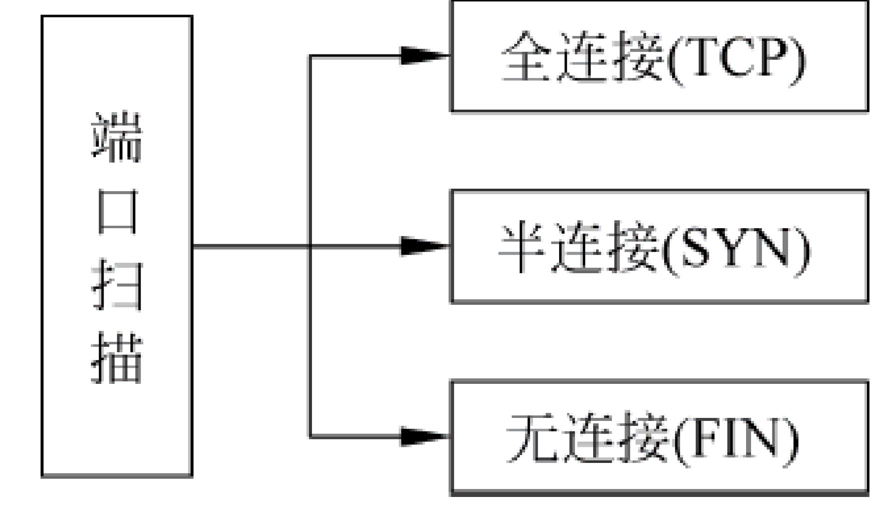


图 3-10　端口扫描原理分类

（1）全连接扫描（TCP 扫描）：这种扫描方法使用三次握手与目标主机建立标准的 TCP 连接，即向对方发送一个正常的 TCP 连接请求，如果存在三次握手，则连接建立。

（2）半连接扫描（SYN 扫描）：若端口扫描没有完成一个完整的 TCP 连接，扫描主机向

目标主机的指定端口发送 SYN 数据段，表示发送建立连接请求。

① 如果目标主机的回应 TCP 报文中 SYN=1，ACK=1，说明该端口是活动的，接着扫描主机传送一个 RST 给目标主机拒绝建立 TCP 连接，从而导致三次握手过程的失败。即建立连接时只完成了前两次握手。

② 如果目标主机回应的是 RST，则表示该端口为“死端口”，这种情况下，扫描主机不用做任何回应。

(3) 无连接扫描(FIN 扫描)：依靠发送 FIN 来判断目标主机的指定端口是否活动。发送一个 FIN=1 的 TCP 报文到一个关闭的端口时，该报文会被丢掉，并返回一个 RST 报文。但是，当发送 FIN 报文到一个活动的端口时，该报文只是简单的丢掉，不会返回任何回应。从 FIN 扫描可以看出，这种扫描没有涉及任何 TCP 连接部分，因此，这种扫描比前两种都安全，可以称为秘密扫描。

4. 漏洞扫描技术

网络扫描的第三阶段采用的漏洞扫描通常是在端口扫描的基础上，对得到的信息进行相关处理，进而检测出目标系统存在的安全漏洞。

漏洞扫描主要通过以下两种方法来检查目标主机是否存在漏洞：

(1) 在端口扫描后得知目标主机开启的端口以及端口上的网络服务，将这些相关信息与网络漏洞扫描系统提供的漏洞库进行匹配，查看是否存在满足匹配条件的漏洞。

(2) 通过模拟黑客的攻击手法，对目标主机系统进行攻击性的安全漏洞扫描，如测试弱口令等，若模拟攻击成功，则表明目标主机系统存在安全漏洞。

3.5 网络攻击

任何以干扰、破坏网络系统为目的的非授权行为都称为网络攻击。黑客进行网络攻击通常分为三大类型：社会工程学攻击、利用型攻击和拒绝服务型攻击。

1. 社会工程学攻击

社会工程学攻击，是一种利用“社会工程学”来实施的网络攻击行为。社会工程学是利用人的本能反应、好奇心、信任、贪便宜等弱点，使用诸如欺骗、伤害等危害手段，获取自身利益的手法。

2. 利用型攻击

利用型攻击是一类试图直接对用户的主机进行控制的攻击，最常见的利用型攻击有物理攻击、暴力攻击、漏洞攻击、缓冲区溢出攻击和木马攻击。

3. 拒绝服务型攻击

拒绝服务型攻击是目前最常见的一种攻击类型。从网络攻击的各种方法和所产生的破坏情况来看，拒绝服务型攻击算是一种很简单，但又很有效的攻击方式。它的目的就是拒绝服务访问，破坏系统的正常运行，最终使网络连接堵塞，或者服务器因疲于处理攻击者发送的数据包而使服务器系统的相关服务崩溃、系统资源耗尽。

3.5.1 社会工程学攻击

社会工程学攻击是利用人们的心理特征骗取用户的信任，获取机密信息、系统设置等不公开的资料，为黑客攻击和病毒感染创造有利条件。

社会工程学攻击与黑客使用的其他技术具有很大的差别，它所研究的对象不是严谨的计算机技术，而是目标网络的人员。社会工程学主要是利用说服或欺骗的方法来获得对信息系统的访问，这种说服和欺骗通常是通过与人交流或其他互动方式实现的。

近年来，更多的黑客转向利用人的弱点即社会工程学方法来实施网络攻击。利用社会工程学手段突破信息安全防御措施的事件，已经呈现出上升甚至泛滥的趋势。

目前社会工程学攻击主要包括两种方式：打电话和伪造 E-mail。

1. 打电话

在社会工程学攻击中有些黑客冒充失去密码的合法雇员，通过这种简单的方法重新获得密码。

2. 伪造 E-mail

使用 telnet，一个黑客可以截获任何一个身份所发送 E-mail 的全部信息，这样的 E-mail 信息是真的，因为它发自于一个合法的用户。一个冒充系统管理员或经理的黑客可以伪造这些信息显得绝对真实的 E-mail，从而较为轻松地获得大量的信息，实施他们的恶意阴谋。

3.5.2 物理攻击

物理攻击是指通过接触到的设备进行攻击。物理攻击有两种方法。

(1) 管理员离开计算机时，没有加密计算机或者直接把管理员登录的计算机借给他人使用时，别人就可以通过工具软件来获得用户名和密码。

(2) 普通用户通过提升权限，获得与管理员相同的权限，达到长期占有计算机的目的，或通过命令进入到某个计算机后，使用命令新建用户名及密码，并提升权限。

到目前为止，任何操作系统都没有本地安全性可言，当本地接触一台计算机时，不管是什么类型的操作系统，都可以轻易地利用一些工具或者系统的一些特性来登录系统。对物理攻击的防范措施主要有：设定计算机屏保和开机密码；计算机需要借出时应该在监督下使用；以及在其他用户使用完后对系统做详细的检查。

3.5.3 暴力攻击

暴力攻击采用字典穷举法(也称暴力法)来破解用户的密码。字典就是一个文本文件，里面包含了所有可能的密码列表。攻击者可以通过一些工具软件，自动地从字典中取出一个单词，作为用户的口令，再输入给远端的主机，申请进入系统；如果口令错误，就按序取出下一个单词，进行下一个尝试，并一直循环下去，直到找到正确的口令或字典的单词试完为止。由于这个破译过程是由计算机程序来自动完成的，所以几个小时就可以把记录在字典里的数十万单词都尝试一遍。也就是说，只有被破解用户的密码存在于字典中，才会被这种方式所找到。千万不要小看这个看上去守株待兔的方法，由于网络上经常有不同的黑客彼此交换字典，因此一份网上流传的字典通常包含了很多黑客累积的经验，对于安全意识不强的用户，破解率是很高的。

1. 暴力攻击类型

目前常用的暴力破解主要包含以下 4 种类型。

1) 词典攻击

因为多数人使用普通词典中的单词作为口令，发起词典攻击通常是较好的开端。词典

攻击使用一个包含大多数词典单词的文件，用这些单词猜测用户口令。

2）强行攻击

许多人认为如果使用足够长的口令，或者使用足够完善的加密模式，就能有一个攻不破的口令。事实上没有攻不破的口令，这只是个时间问题。如果有速度足够快的计算机能尝试字母、数字、特殊字符等所有的组合，将最终能破解所有的口令。这种类型的攻击方法叫作强行攻击。使用强行攻击，先从字母 a 开始，尝试 aa、ab、ac 等，然后再尝试 aaa、aab……以此类推下去。

3）组合攻击

词典攻击只能发现词典单词口令，但是速度快。强行攻击能发现所有的口令，但是破解时间很长。在公司里，很多管理员要求员工设置口令时使用字母和数字组合，一些员工的对策是在口令后面添加几个数字。如把口令 computer 变成 computer123，实际上这样的口令很弱。有一种攻击使用词典单词，但是在单词尾部串接几个字母和数字，这就是组合攻击。它基本上介于词典攻击和强行攻击之间。图 3-11 是一个简单的组合攻击字典文件。



图 3-11　字典文件

4）社会工程学字典攻击

如果黑客从侧面了解到该服务器所属单位的电话号码范围、街道号、门牌号、网络管理员的手机号、生日等，就会以这些数据为基准参数制造黑客字典。因为很多人为了记忆简便，都会利用自己的一些常用信息作为密码，所以就导致了字典攻击的可能性。利用对目标用户本人的了解，可以使用社会工程学来生成字典，再利用该字典进行攻击，这个字典的成功率会比盲目地使用一个字典的成功率高。图 3-12 是一个社会工程学字典生成器主界面。

社会工程学字典

用户名(拼音)：　用户出生日期：示例：19841010　用户邮箱名：
用户手机号：　用户座机号：　用户网名(英文/拼音)：
用户名(五笔)：　用户邮编：　用户QQ号：
用户网址：　用户网站成立日期：　所属组织名(拼音)：
常用密码：　习惯用的字符/英文/数字：　女友/妻子名字(拼音)：
女友/妻子电话：　女友/妻子出生日期：　女友/妻子名字(五笔)：
女友/妻子网名：　用户最好的朋友名(拼音)：　用户常用注册名(拼音)：
生成密码字典

图 3-12　社会工程学字典生成器主界面

2. 暴力攻击的防御

暴力攻击的防御方法如下：

(1) 不管是服务器还是客户计算机，尽量减少账户的数量；

(2) 所有账户的密码必须足够复杂，一般约定普通客户计算机上的账户密码最小长度为6位，服务器上的账户密码最小长度为8位；

(3) 密码不要使用与单位或个人有关的信息构成；

(4) 根据现在通用的密码暴力猜测算法，可以反向思考，加大黑客的破解难度，如可以用大写字母开头构造密码，或者以特殊字符开头构造密码；

(5) 密码中不要包含英文单词，英文单词是字典攻击的猜测范围，破解成功率很高；

(6) 密码中不要使用连续的字符或者字母；

(7) 密码必须强行设置策略实现至少40天更新一次，更新后的密码与更新前的密码不要类似，更加不要使用曾经使用过的密码；

(8) 设置服务器或者客户计算机的操作系统密码尝试次数。

3.5.4 漏洞攻击

漏洞一词是从英文单词vulnerability翻译而来的，原词应译为"脆弱性"，但是中国的技术人员已经更愿意接受"漏洞"这一通俗化的解释。从众多报刊杂志或者网络资源中，人们或许已经对计算机系统的"漏洞"这个概念有了一个感性的理解。确实，这里的"漏洞"并不是一个物理上的概念，它是指计算机系统具有的某种可能被入侵者恶意利用的属性。

简单地说，计算机漏洞是系统的一组特性。恶意的入侵者能够利用这组特性，通过已授权的手段和方式获取对资源的未授权访问，或者对系统造成损害。这里的漏洞既包括单个计算机系统的漏洞，也包括计算机网络系统的漏洞。当系统的某个漏洞被入侵者渗透而造成泄密时，其结果就称为一次安全事件。

1. 存在漏洞的原因

从技术角度而言，漏洞的来源主要有以下几个方面：

(1) 软件或协议设计时的瑕疵。协议定义了网络上计算机会话和通信的规则，如果在协议设计时存在瑕疵，那么无论实现该协议的方法多么完美，它都存在漏洞。

(2) 软件或协议实现中的弱点。即使协议设计得很完美，实现协议的方式仍然可能引入漏洞。

(3) 软件本身的瑕疵。例如，没有进行数据内容和大小的检查，不能正常处理资源耗尽的情况等，攻击者通过渗透这些漏洞，即使不具有特权账号，也可能获得额外的、未授权的访问。

(4) 系统和网络的错误配置。这一类漏洞并不是由协议或软件本身的问题造成的，而是由服务和软件的不正确部署和配置造成的。

2. 公开的计算机漏洞信息

公开漏洞可以促使提供软件或硬件的厂商更快地解决问题，也可以让系统管理员更有针对性地对自己管理的系统进行配置和管理。多年的实践也使人们逐渐认识到，建立在漏洞公开基础之上的安全才是更可靠的安全。因特网上已经有许多关于各种漏洞的描述和与此相关的数据库。下面是一些比较权威的漏洞信息资源。

(1) 通用漏洞和曝光。通用漏洞和曝光(CVE)是一个公共安全漏洞和曝光信息的标准

化名字列表，它致力于为所有公开的漏洞和安全曝光名称制定标准化的工作。CVE 是一个字典而不是数据库，它的目标是使不同的漏洞数据库共享数据和搜索信息变得更加容易。目前已经有 200 多个组织、产品和安全警告提供服务实现了“CVE 兼容”。

（2）CERT/CC 漏洞信息数据库。CERT/CC 漏洞数据库也是一个 CVE 兼容的数据库。它可以通过名字、ID 号、CVE 名字、发布日期、严重性等字段检索漏洞信息。

3.5.5 缓冲区溢出攻击

目前最流行的一种攻击技术就是缓冲区溢出攻击。当目标操作系统收到了超过它能接收的最大信息量时，将发生缓冲区溢出。这项攻击对技术要求比较高，但是攻击的过程却非常简单。

1. 缓冲区溢出

缓冲区溢出是指当计算机程序向缓冲区内填充的数据位数超过缓冲区本身的空间时，溢出的数据覆盖在合法数据上。理想情况是，程序检查数据长度并且不允许输入超过缓冲区长度的字符串。大多数程序都会假设数据长度总是与所分配的存储空间相匹配，这就为缓冲区溢出埋下了隐患。操作系统所使用的缓冲区又被称为堆栈，在各个操作进程之间，指令被临时存储在堆栈中，堆栈也会出现缓冲区溢出。

缓冲区溢出的原理很简单，如下所示。

```
void function (char * str)
{
    char buff[16];
    strcpy(buff,str);
}
```

程序中利用 strcpy()函数将 str 中的内容复制到 buff 中，只要 str 的长度大于 16，就会造成缓冲区溢出，存在类似 strcpy()函数这种问题的 C 语言函数还有很多。

当一个超长的数据进入到缓冲区时，超出部分就会被写入其他缓冲区，其他缓冲区存放的可能是数据、下一条指令的指针或者是其他程序的输出内容，这些内容都被覆盖或者破坏掉了。可见一小部分数据或者一套指令的溢出就可能导致一个程序或者操作系统崩溃。

缓冲区溢出是由编程错误引出的。如果缓冲区被写满，而程序没有去检查缓冲区边界，也没有停止接收数据，这时缓冲区溢出就会发生。缓冲区溢出之所以泛滥，是由于开放源代码程序的本质决定的。标准 C 语言具有许多复制和添加字符串的函数，这使得标准 C 语言很难进行边界检查。一般情况下，覆盖其他数据区的数据是没有意义的，最多造成应用程序错误，但是，如果输入的数据是经过黑客精心设计的，覆盖缓冲区的数据恰恰是黑客或者病毒的攻击程序代码，一旦多余字节被编译执行，黑客或者病毒就有可能为所欲为，获取系统的控制权。

2. 缓冲区溢出的防御

缓冲区溢出是目前导致“黑客”型病毒横行的主要原因。从“红色代码”到 Slammer，再到“冲击波”，都是利用缓冲区溢出漏洞的典型病毒案例。缓冲区溢出是一个编程问题，防止利用缓冲区溢出发起的攻击，关键在于程序开发者在开发程序时仔细检查溢出情况，不允许数据溢出缓冲区。此外，用户需要经常登录操作系统和应用程序提供商的网站，跟踪公布的

系统漏洞，及时下载补丁程序，弥补系统漏洞。因此，缓冲区溢出的防御方法大致可以划分为以下两类。

(1) 编译时防御，目标是加固程序来抵抗在新程序中的攻击。

编译时防御，是指在进行编译时通过检测程序防止或侦测缓冲区溢出。完成该防御的可能性关键在于选择一种不允许缓冲区溢出的高级语言，鼓励使用安全的编码技术，使用安全的标准库，或者包含用来检测栈帧是否被破坏的附加代码。

(2) 运行时防御，目标是在现有的程序中检测和终止攻击。

就像我们已经注意到的那样，大多数编译时防御的方法需要对现有的程序重新编译。因此，人们有了对运行时防御的兴趣，像操作系统通过更新来对存在漏洞的程序提供保护一样，运行时防御也能如此配置。

3.5.6 木马攻击

木马攻击是黑客最常用的攻击方法，木马的危害性在于它对计算机系统强大的控制和破坏能力，如窃取密码、控制系统操作、进行文件操作等，一台计算机一旦被一个功能强大的木马植入，攻击者就可以像操作自己的计算机一样控制这台计算机，远程监控这台计算机上的所有操作。

木马全称“特洛伊木马”，英文为 Trojan Horse，它来源于古希腊故事。有一次，古希腊大军围攻特洛伊城，久攻不下。于是古希腊谋士献计制造一只高二丈的大木马假装作战神马，随后在攻击数天后假装兵败，留下木马拔营而去。城中得到解围的消息，举城欢庆，并把这个奇异的战利品搬入城内，当全城军民尽入梦乡时，藏于木马中的将士从木马中打开密门而下，打开城门引入外兵，攻下特洛伊城。这就是“特洛伊木马”的来历。计算机界把伪装成良性程序的文件形象地称为“木马”。

木马主要有以下特点。

(1) 伪装性，木马总是伪装成其他程序来迷惑管理员。

(2) 潜伏性，木马能够毫无声响地打开端口等待外部连接。

(3) 隐蔽性，木马的运行隐蔽，甚至使用进程查看器都看不出。

(4) 不易删除，计算机一旦中了木马，最省事的方法就是重装系统。

(5) 通用性，即使远程主机是 Windows 98 系统，入侵者也可以实现远程控制。

木马与后门的区别：本质上，木马和后门都有提供网络后门的功能，但是木马的功能稍微强大一些，一般还有远程控制的功能，而后门程序的功能比较单一，只是方便客户端能够登录对方的主机。

1. 木马分类

常见的木马主要可以分为以下 8 种类型。

1) 破坏型木马

破坏型木马唯一的功能就是破坏并且删除文件，它能自动删除目标计算机上的 DLL、EXE 文件，所以非常危险，一旦被感染就会严重威胁计算机的安全。

2) 密码发送型木马

密码发送型木马是专门为了盗取被感染的计算机上的密码编写的，木马一旦执行，就会自动搜索内存、临时文件夹及各种敏感文件，一旦搜索到有用的密码，木马就会利用免费的

电子邮件服务将密码发送到指定的邮箱，达到获取密码的目的。这类木马大多使用25号端口发送E-mail，它们大多会在每次Windows重启时重新运行，其目的是找到所有隐藏密码并且在受害者不知道的情况下把密码发送到指定的邮箱。如果目标计算机有隐藏密码，这些木马是很危险的。

3）远程访问型木马

最有代表性的远程访问型木马是特洛伊木马，如果客户知道了服务端的IP地址，只需运行服务端程序就可以实现远程控制。

4）键盘记录木马

这种特洛伊木马是非常简单的，它只做一件事情，就是记录被攻击者的键盘敲击并且在LOG文件里查找密码，这种特洛伊木马随着Windows的启动而启动。它们分为在线记录和离线记录，分别记录在线和离线状态下敲击键盘时的按键情况。从这些按键中很容易就会得到密码等有用信息，当然对于这种类型的木马，邮件发送功能也是必不可少的。

5）DoS攻击木马

随着DoS攻击应用得越来越广泛，被用作DoS攻击的木马也越来越流行起来。当一台计算机被入侵并被种上了DoS攻击木马，那么日后这台计算机就成为DoS攻击者的最得力的助手了。攻击者控制的“肉鸡”数量越多，发动DoS攻击取得成功的概率就越大。所以，这种木马的危害不是体现在被感染的计算机上，而是体现在攻击者可以利用它来攻击一台又一台计算机，给网络造成很大的伤害和损失。

还有一种类似DoS攻击的木马称为邮件炸弹木马，一旦计算机被感染，木马就会随机生成各种各样主题的信件，对特定的邮箱不停地发送邮件，一直到对方瘫痪，不能接受邮件为止。

6）代理木马

黑客在入侵的同时掩盖自己的足迹，谨防别人发现自己的身份是非常重要的，因此，给被控制的“肉鸡”种上代理木马，让其变成攻击者发动攻击的跳板就是代理木马最重要的任务。通过代理木马，攻击者可以在匿名的情况下使用Telnet等程序，从而隐藏自己踪迹。

7）FTP木马

这种木马可能是最简单和最古老的木马，它的唯一功能就是打开21端口，等待用户连接。现在新FTP木马还加上了密码功能，因此只有攻击者本人才知道正确的密码，从而进入对方计算机。

8）程序杀手木马

上面的木马功能虽然形形色色，不过要到对方计算机上发挥自己的作用，还要通过防木马软件这一关才行。常见的防木马软件有ZoneAlarm、Norton Anti-Virus等。程序杀手木马的功能就是关闭对方计算机上运行的这类程序，让其他的木马更好地发挥作用。

2. 木马连接方式

1）传统连接方式

传统连接方式即C/S连接方式，在这种连接方式下，远程主机开放监听端口等待外部连接，成为服务端。当入侵者需要与远程主机建立连接的时候，便主动发出连接请求，从而建立连接，建立过程如图3-13所示。

这种连接需要服务端开放端口等待连接，需要客户端知道服务端的IP地址与服务端口号。因此，传统连接不适合与动态IP地址或局域网内主机建立连接。

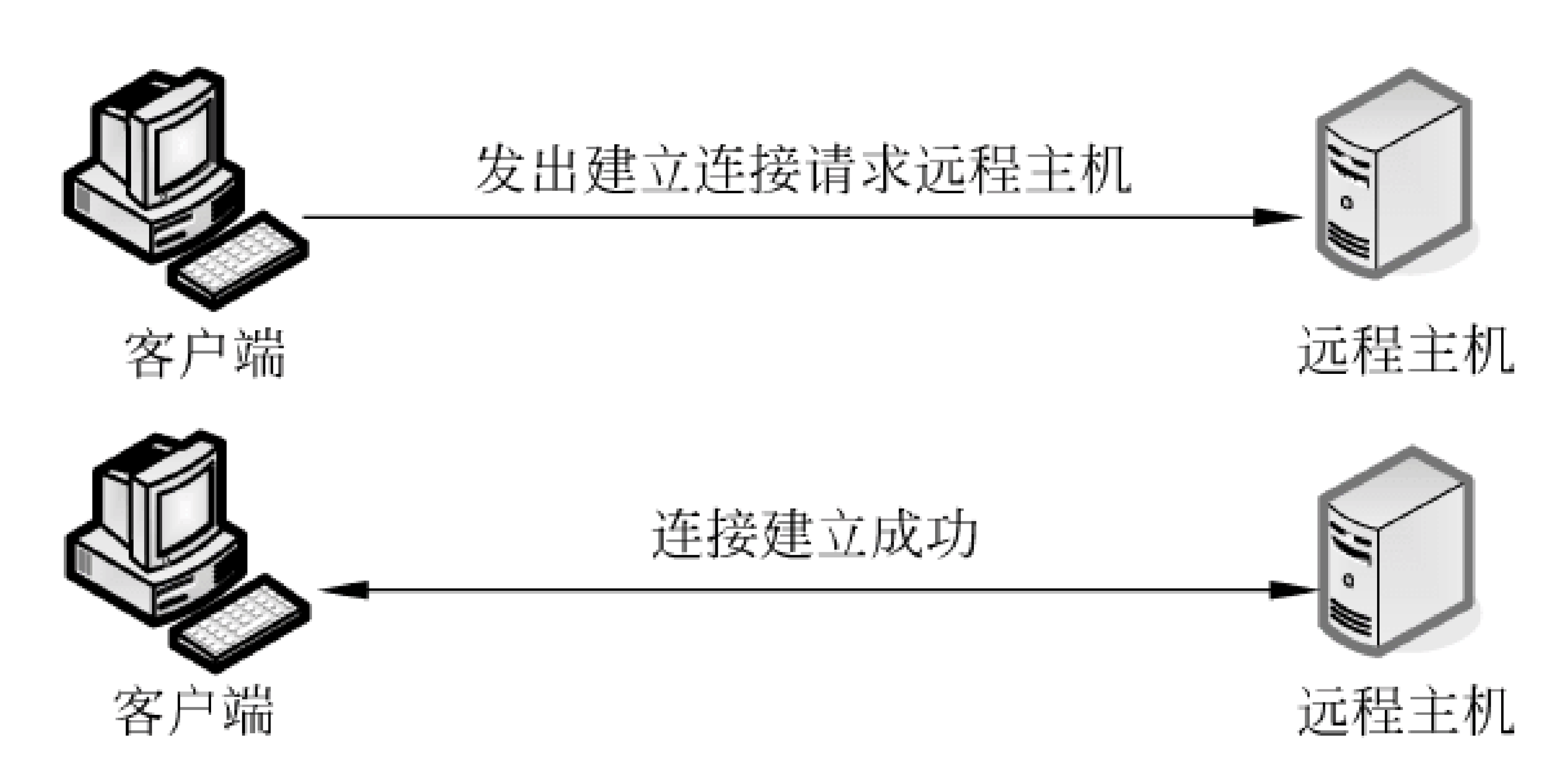


图 3-13　传统连接方式

2）反弹端口连接方式

反弹端口连接方式中连接的建立不再由客户端主动要求连接，而是由服务端来完成，这种连接过程恰恰与传统连接方式相反。当远程主机安装木马后，由远程主机主动寻找客户端建立连接，客户端则开放端口等待连接，具体建立过程如图 3-14 所示。

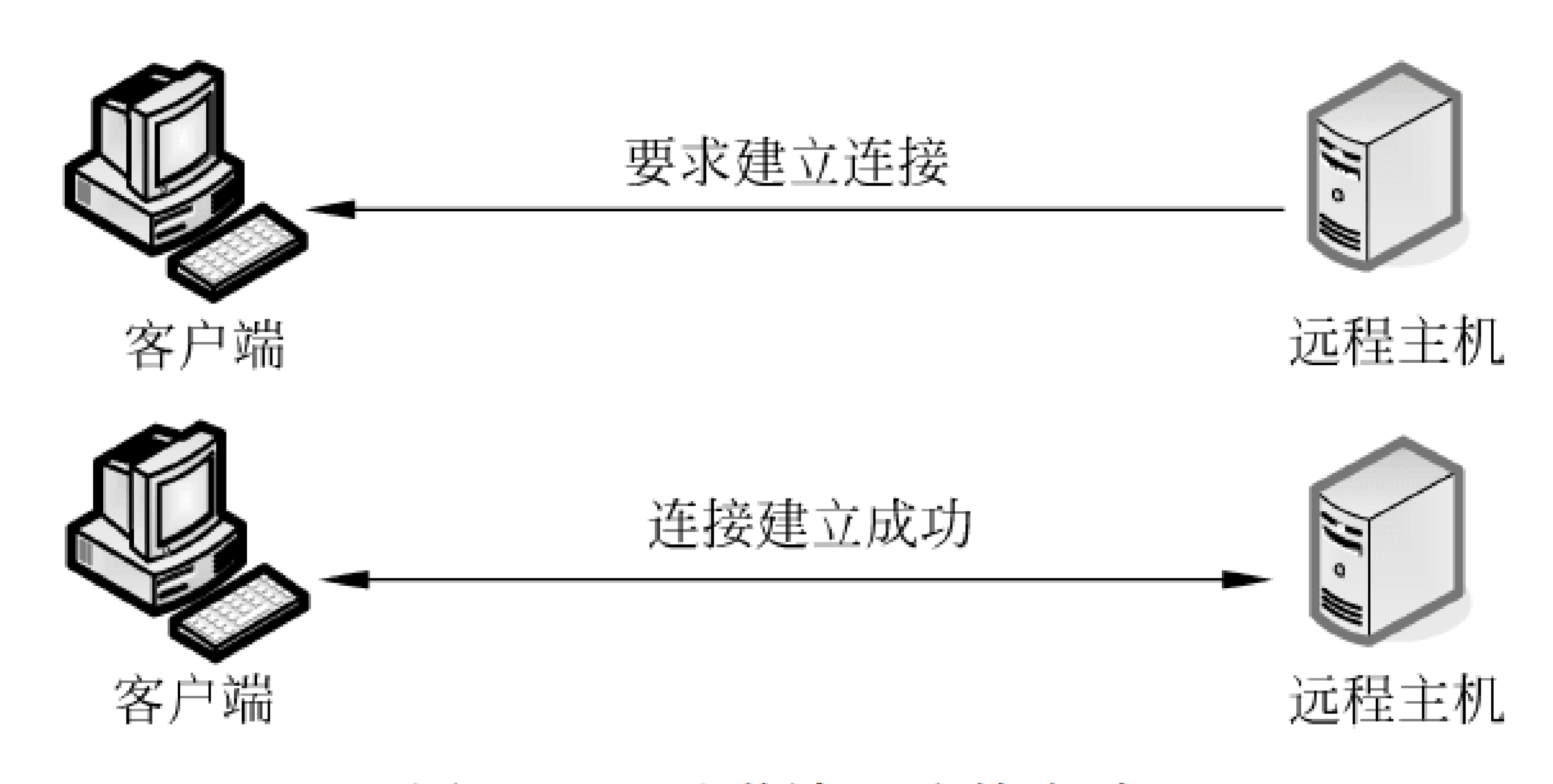


图 3-14　反弹端口连接方式

3. 木马防御

使用以下方法进行防御，基本上可以阻止基于木马的入侵。

1）显示文件扩展名

文件扩展名是文件格式和功能的代表，通过文件扩展名，管理员一眼就能认出文件的真正身份，例如，.exe 代表可执行文件，.jpg 代表图形文件、.txt 代表文本文件，.htm 代表网页文件等。知道了文件的扩展名，再看文件的图标，如果它们之间的对应不一致，如文件扩展名是.exe，但却使用了.jpg 的图标，那么就说明这个文件被修改过，这样的文件大多是木马。

2）不打开任何可疑文件、文件夹、网页

不只是执行扩展名为.exe、.bat 的文件名有被攻击的危险，打开网页和文件夹也都有危险，因此，只有尽量不打开任何可疑文件、文件夹、网页，才能避免被种植木马。

3）升级 IE

很多木马是利用了 IE 的漏洞，所以要经常升级 IE。

4）常开病毒防火墙

由于病毒防火墙比较占系统资源，容易造成系统运行缓慢，因此许多管理员不喜欢开病毒防火墙，而是认为新下载的文件进行病毒扫描就足够了。但是需要注意的是，仅仅使用杀毒软件对文件进行扫描是远远不能实现安全目的的，病毒防火墙能够对系统进行实时监控，及时发现活动的木马并把它杀死。

5）常开网络防火墙

使用网络防火墙并进行相应的设置，这样一来，即使计算机真的中了木马程序，防火墙也可以拦截大多数木马的连接。

3.5.7 拒绝服务攻击

1. DoS 攻击

拒绝服务（Denial-of-Service，DoS）攻击是一种针对某些服务可用性的攻击。从计算机和通信安全的角度讲，DoS 攻击一般攻击目标系统的网络服务，通过攻击其网络连接来实现。这种针对服务可用性的攻击不同于其他传统意义上的不可抗力产生的攻击，它是通过造成 IT 基础设备的损害或毁坏而导致服务能力的丧失。

NIST 计算机安全事故处理指南（NIST Computer Security Incident Handling Guide）中对 DoS 攻击给出的定义如下：拒绝服务是一种通过耗尽 CPU、内存、带宽以及磁盘空间等系统资源，来阻止或削弱对网络、系统或应用程序的授权使用的行为。

由上述定义可知，可作为 DoS 攻击对象的资源有下面几类。

1）网络带宽

网络带宽与连接服务器和因特网的网络链路的容量相关。对于大部分机构来说，网络带宽指的是连接到其网络服务提供商的链路容量，如图 3-15 给出的网络实例所示。通常这个连接的容量低于 ISP 路由器内部以及 ISP 路由器之间的链路容量，这就意味着可能会发生这样的情况：经过具有更高容量的链路而到达 ISP 路由器的通信量要高于到机构的链路的通信量。在这种情况下，ISP 路由器只能发送链路所能承载的最大流量，对于超出的流量

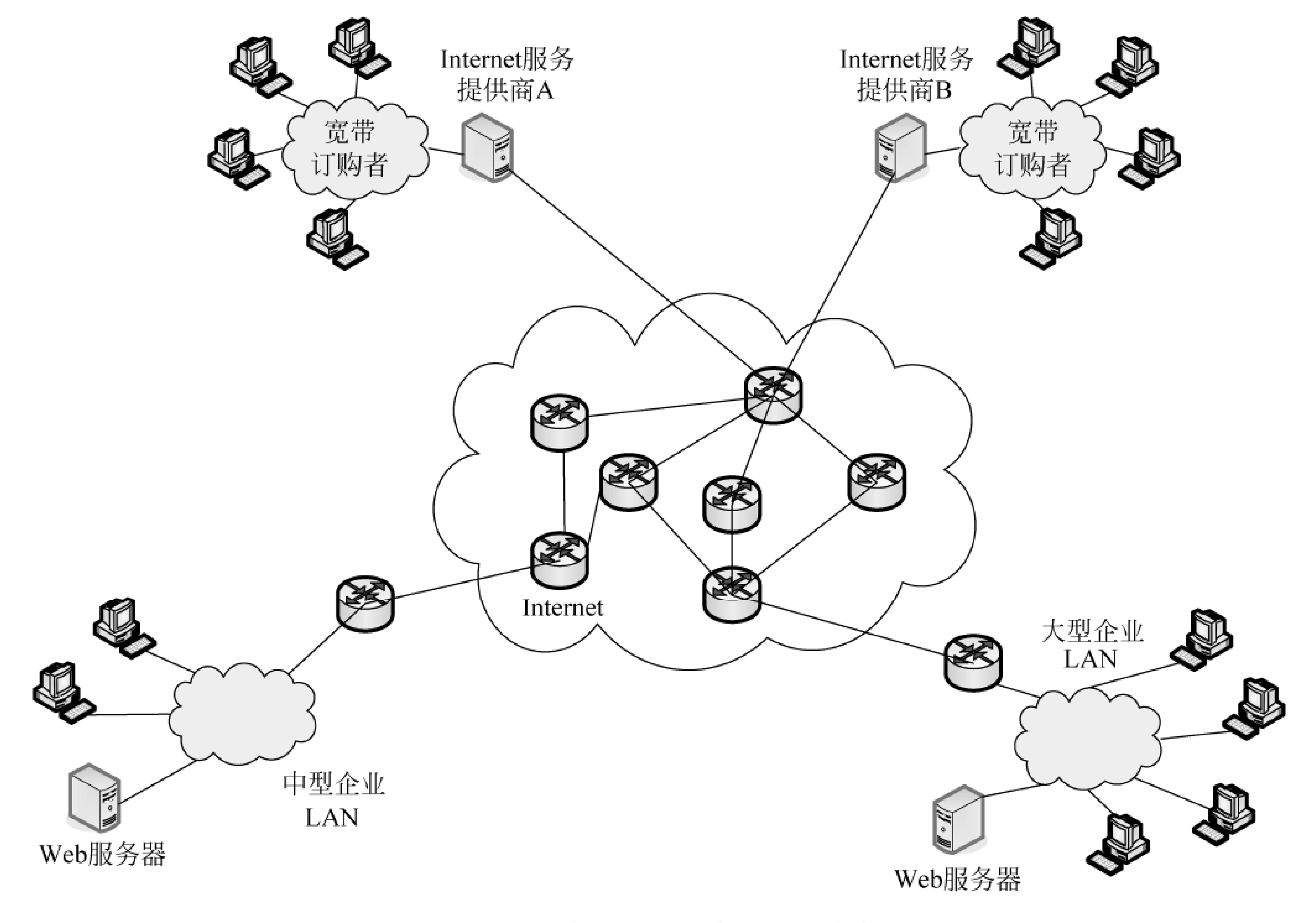


图 3-15 说明 DoS 攻击的网络实例

必须丢弃。在正常网络运行环境下，正常用户的超负荷访问同样会使得服务器网络繁忙。那么这些正常用户当中就会随机地有一部分不能得到服务器的响应，对于一个已经超负荷的 TCP/IP 网络连接来说，服务器不可用也是预料之中的。但在 DoS 攻击的情况下，攻击者直接地或间接地制造出大量的恶意流量发往目标服务器。这种攻击流量相比任何的合法流量来说是压倒性的，从而有效地拒绝了合法用户对服务器的访问。

2）系统资源

针对系统资源的 DoS 攻击，是通过使用某些特殊数据包来触发系统的网络处理软件的缺陷，从而导致系统崩溃。如果受到这种 DoS 攻击，除非管理员重新启动网络处理程序，否则服务器将无法再通过网络处理程序来提供网络服务。例如，经典的死亡之 ping 和泪滴攻击都是这种类型的攻击，它们主要是针对早期的 Windows 9x 操作系统。

3）应用资源

针对特定应用服务程序的攻击一般使用一定数量的合法请求，而每个合法请求都会明显地消耗掉服务器上的系统资源，从而达到限制服务器响应其他合法用户请求的目的。例如，某 Web 服务器可能会提供数据库查询服务，如果能够构造出一个巨大的、高代价的查询请求，那么攻击者就能够向服务器提出大量的这类查询请求。这样就会限制 Web 服务器响应其他合法用户的查询请求。

2. DoS 攻击原理

DoS 攻击的基本原理是使被攻击服务器充斥大量要求回复的信息，消耗网络带宽或系统资源，导致网络或系统不胜负荷以至于瘫痪，而停止提供正常的网络服务。

要对服务器实施拒绝服务攻击，有两种方式：

（1）迫使服务器的缓冲区满载，不接收新的请求；

（2）使用 IP 欺骗，迫使服务器把合法用户的连接复位。影响合法用户的连接，这也是 DoS 攻击实施的基本思想。

为便于理解，介绍一个简单的 DoS 攻击基本过程，如图 3-16 所示。

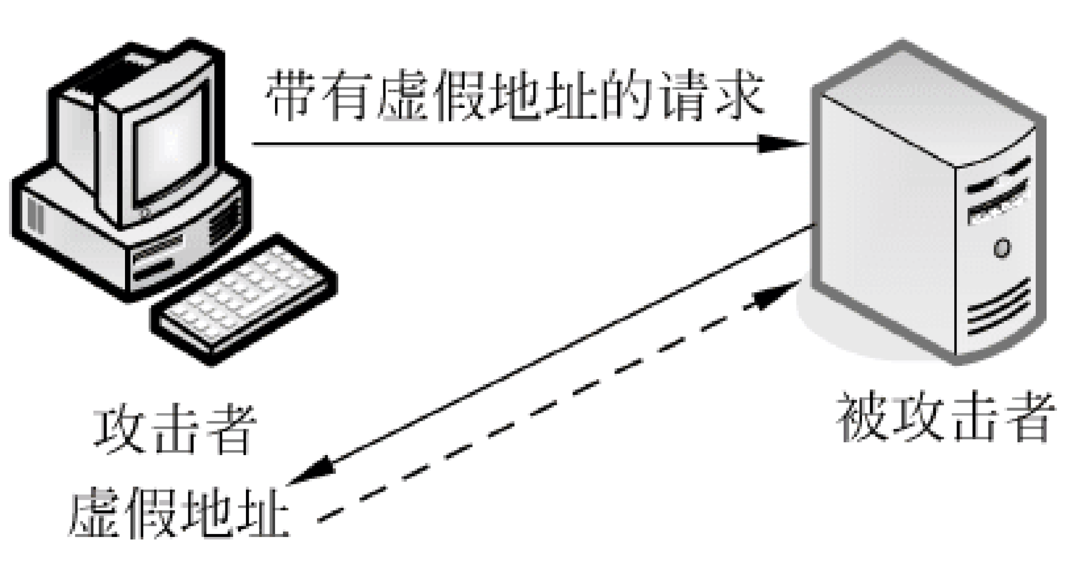


图 3-16 一个简单的 DoS 攻击的基本过程

攻击者先向被攻击者发送众多带有虚假地址的请求，被攻击者发送回复信息后等待回传信息，由于是伪造地址，所以被攻击者一直等不到回传信息，分配给这次请求的资源就始终不被释放。当被攻击者等待一段时间后，连接会因超时被切断，攻击者会再度传送一批伪地址的新请求，这样反复进行，被攻击者的资源将被耗尽，最终导致被攻击者主机瘫痪。

3. DoS 攻击类型

DoS 攻击从攻击目的和手段上主要分为以下一些类型，它们以不同的方式对目标网络造成破坏。

1）带宽耗用 DoS 攻击

最阴险的 DoS 攻击是带宽耗用攻击。它的本质就是攻击者消耗掉通达某个网络的所有可用的带宽。这种攻击可以发生在局域网上，不过更常见的是攻击者远程消耗资源。为了达到这一目的，一种方法是攻击者通过使用更多的带宽造成受害者网络的拥塞，另一种方

法是攻击者通过征用多个站点，集中拥塞受害者的网络连接来达到 DoS 攻击效果。

2）资源衰竭 DoS 攻击

资源衰竭攻击与带宽耗用攻击的差异在于前者集中于系统资源的消耗而不是网络资源的消耗。一般来说，它涉及诸如 CPU 利用率、内存、文件系统和系统进程总数之类系统资源的消耗。攻击者往往拥有一定数量系统资源的合法访问权，然后，攻击者会滥用这种访问权消耗额外的资源，这样，系统或合法用户被剥夺了原来享有的资源，造成系统崩溃或可利用资源耗尽。

3）编程缺陷 DoS 攻击

部分 DoS 攻击并不需要发送大量的数据包来进行攻击。编程缺陷攻击就是利用应用程序、操作系统等在处理异常条件时的逻辑错误实施的 DoS 攻击。攻击者通常向目标系统发送精心设计的畸形分组来试图导致服务的失效和系统的崩溃。

4）基于路由的 DoS 攻击

在基于路由的 DoS 攻击中，攻击者操纵路由表项以拒绝向合法系统或网络提供服务。诸如路由信息协议和边界网关协议之类较早版本的路由协议没有或只有很弱的认证机制，这就给攻击者变换合法路径提供了良好的前提，它们往往通过假冒源 IP 地址就能创建 DoS 攻击。这种攻击的后果是受害者网络的分组经由攻击者的网络路由，或者被路由到不存在的黑洞网络上。

5）基于 DNS 的 DoS 攻击

基于 DNS 的攻击与基于路由的 DoS 攻击类似。大多数的 DNS 攻击会将虚假的地址信息发送给受害者的域名服务器高速缓存，这样，当用户请求某 DNS 服务器执行查找请求的时候，攻击者就达到了把它们重定向到自己喜欢的站点上的效果。

4. 分布式拒绝服务攻击

DDoS 全名是 Distributed Denial of Service（分布式拒绝服务攻击），很多 DoS 攻击源一起攻击某台服务器就组成了 DDoS 攻击，DDoS 最早可追溯到 1996 年最初，在中国开始频繁出现于 2002 年，2003 年已经初具规模。DDoS 攻击是利用一批受控制的机器向一台机器发起攻击，这种攻击来势迅猛，令人难以防备，且具有较大的破坏性。

一个比较完善的 DDoS 攻击体系分成 4 大部分，如图 3-17 所示。

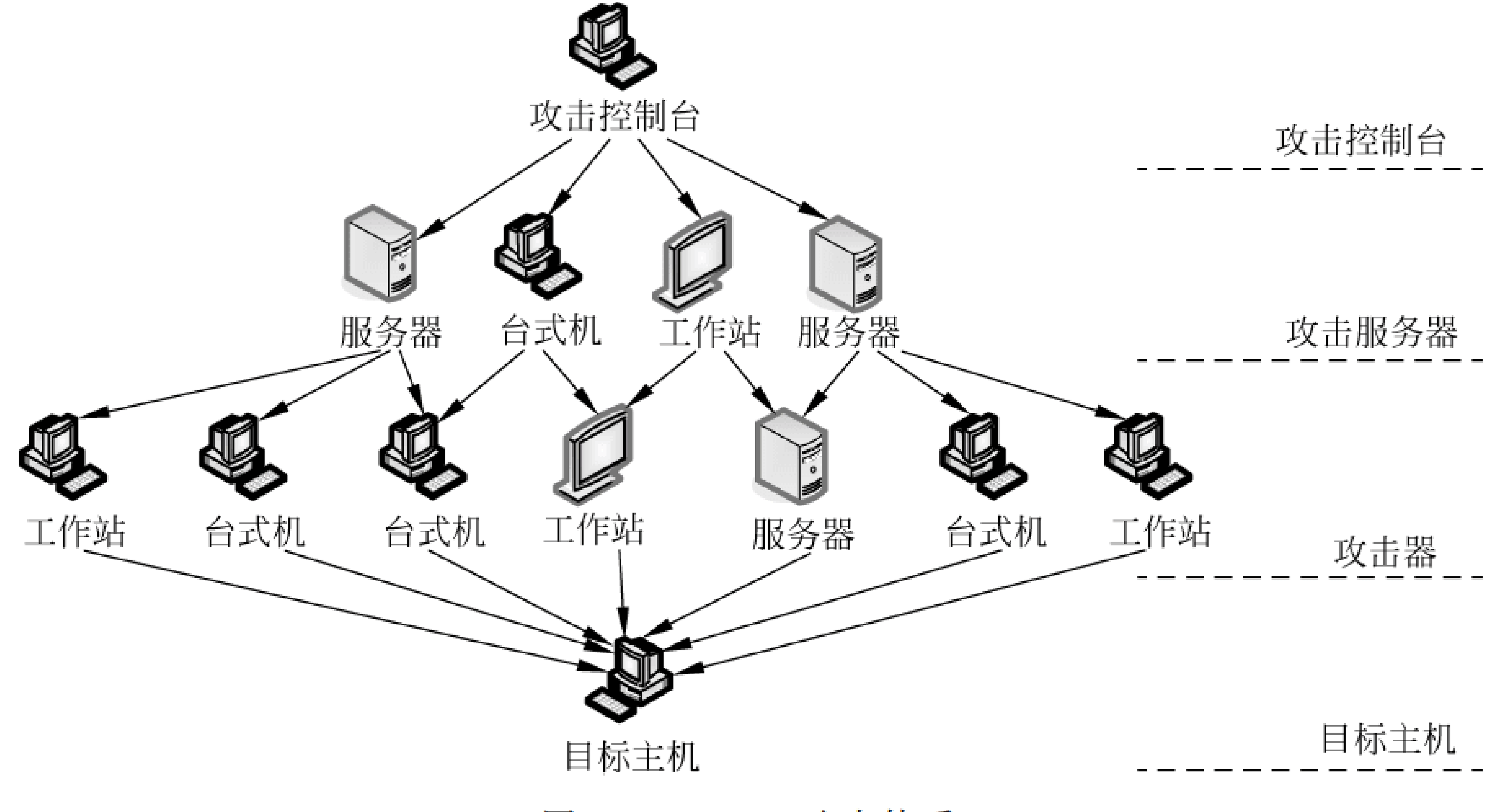


图 3-17　DDoS 攻击体系

（1）攻击控制台：黑客所用的主机，也称为攻击者。它操纵整个攻击过程，向攻击服务器发送攻击命令。

（2）攻击服务器：是攻击者非法侵入并控制的一些主机，这些主机分别控制大量的代理攻击主机。其上面安装特定的程序，可以接收攻击者发来的特殊指令，并且可以把这些指令发送到攻击器上。

（3）攻击器：也是攻击者侵入并控制的一批主机，其上面运行攻击程序，接收和运行攻击服务器发来的命令。

（4）目标主机：被攻击的受害者。

先来看一下最重要的攻击服务器和攻击器，它们分别用作控制和实际发起攻击。请注意攻击服务器与攻击器的区别，对目标主机来说，DDoS 的实际攻击包是从攻击器傀儡机上发出的，攻击服务器只发布命令而不参与实际的攻击。对于攻击服务器和攻击器，攻击控制台有控制权或者部分控制权，并把相应的 DDoS 程序上传到这些平台上，这些程序与正常的程序一样运行并等待来自黑客的指令，通常它还会利用各种手段隐藏自己不被别人发现。在平时，这些攻击服务器并没有什么异常，只是一旦黑客连接到它们进行控制并发出指令，攻击服务器就成为害人者去发起攻击了。

为什么黑客不直接去控制攻击器，而要从攻击服务器上转一下呢？从攻击者的角度来说，他肯定不愿意被发现，而攻击者使用的傀儡机越多，他实际上提供给受害者的分析依据就越多。在占领一台计算机后，高水平的攻击者会首先做两件事：第一，考虑如何留好后门；第二，考虑如何清理日志。但是在攻击器上清理日志实在是一项庞大的工程，即使在很好的日志清理工具的帮助下，黑客想完全清除日志也是比较困难的。这就导致了有些攻击器清除日志不是很干净，通过它上面的线索能找到控制它的上一级计算机，上级计算机如果是黑客自己的机器，那么他就会被查找出来。但如果这是攻击服务器的话，黑客自身还是安全的。攻击服务器的数目很少，一般一台就可以控制几十台攻击器，清理一台攻击服务器的日志对黑客来讲就容易多了，这样从攻击服务器再找到黑客的可能性也大大降低。

5. DDoS 攻击过程

DDoS 攻击的过程可以描述如下：

（1）搜集了解目标的情况。了解被攻击目标主机的数据、地址情况，目标主机的配置、性能，以及目标主机的带宽，从目标主机中找到可能成为傀儡机的主机。

（2）占领傀儡机。傀儡机选择链路状态好、性能好、安全管理水平差的主机。首先采用扫描手段，随机或者是有针对性地利用扫描器去发现互联网上那些有漏洞的主机，如程序的溢出漏洞、数据库漏洞等；随后尝试入侵，一旦入侵成功，把 DDoS 攻击用的程序上传过去，一般是利用 FTP。在攻击器上，会有一个 DDoS 的发包程序，攻击者就是利用它来向目标主机发送恶意攻击包。

（3）实际攻击。经过前两个阶段的精心准备，就可以瞄准目标准备攻击了。攻击者登录到作为攻击服务器的傀儡机，向所有的攻击器发出 DDoS 攻击命令，这时候埋伏在攻击器中的 DDoS 攻击程序就会响应攻击服务器的命令，一起向目标主机或设备高速发送大量的数据包，导致服务停止、死机或连接线路拥塞中断。

6. DDoS 防御方法

1）定期扫描

要定期扫描现有的网络主节点，清查可能存在的安全漏洞，对新出现的漏洞及时进行清

理。骨干节点的计算机因为具有较高的带宽，是黑客利用的最佳位置，因此对这些计算机本身加强安全配置是非常重要的。而且连接到网络主节点的都是服务器级别的计算机，所以定期扫描漏洞就变得更加重要了。

2）采用高性能的网络设备

首先要保证网络设备不能成为瓶颈，因此选择路由器、交换机、硬件防火墙等设备的时候要尽量选用知名度高、口碑好的产品。假如和网络提供商有特殊关系或协议的话，当大量攻击发生时请他们在网络接点处做一下流量限制来对抗某些种类的 DDoS 攻击是非常有效的。

3）尽量避免 NAT 的使用

无论是路由器还是硬件防护墙设备要尽量避免采用网络地址转换 NAT 的使用，因为采用此技术会大幅降低网络通信能力。原因是 NAT 需要对地址来回转换，转换过程中需要对网络包校验和进行计算，因此浪费了很多 CPU 的时间，但在必须使用 NAT 时，那就只能如此了。

4）充足的网络带宽保证

网络带宽直接决定了能抵抗攻击的能力，假若仅仅有 10M 带宽的话，无论采取什么措施都很难对抗现在的 SYNFlood 攻击，目前至少要选择 100M 的共享带宽，最佳选择是使用 1000M 的共享带宽。但需要注意的是，主机上的网卡是 1000M 的并不意味着它的网络带宽就是千兆的，若把它接在 100M 的交换机上，它的实际带宽不会超过 100M，而且接在 100M 的带宽上也不等于就有了百兆的带宽，因为网络服务商很可能会在交换机上限制实际带宽为 10M。

5）在骨干节点配置防火墙

防火墙本身能抵御 DDoS 攻击和其他一些攻击。在发现受到攻击的时候，可以将攻击导向一些牺牲主机，这样可以保护真正的主机不被攻击。

6）过滤不必要的服务和端口

过滤不必要的服务和端口，只开放服务端口成为目前很多服务器的流行做法，如 WWW 服务器只开放 80 端口而将其他所有端口关闭或在防火墙上做阻止策略。

7）检查访问者的来源

使用 Unicast Reverse Path Forwarding 等通过反向路由器查询的方法检查访问者的 IP 地址是否是真，如果是假的，将予以屏蔽。许多黑客在攻击时常采用假 IP 地址的方式迷惑用户，很难查出它来自何处。因此，利用 Unicast Reverse Path Forwarding 可减少假 IP 地址的出现，有助于提高网络安全性。

8）限制 SYN/ICMP 流量

用户应在路由器上配置 SYN/ICMP 的最大流量来限制 SYN/ICMP 包所能占有的最高带宽，当出现的较大流量超过 SYN/ICMP 的限定时，说明不是正常的网络访问，而是有黑客入侵。早期限制 SYN/ICMP 流量是最好的防范 DoS 的方法，虽然目前该方法对于 DDoS 效果不太明显了，不过仍然能够起到一定的作用。

7. DDoS 防护部署

1）串行部署防御 DDoS 攻击

串行部署防御模式主要应用在企业网络中，在网络的出口或要保护的目标地址前进行部署，提供串行的保护形式，如图 3-18 所示。

此种部署模式不需要 DDoS 攻击检测器，而是直接将防护设备部署在需要保护的设备前面，利用设备的识别能力，直接过滤攻击流量。

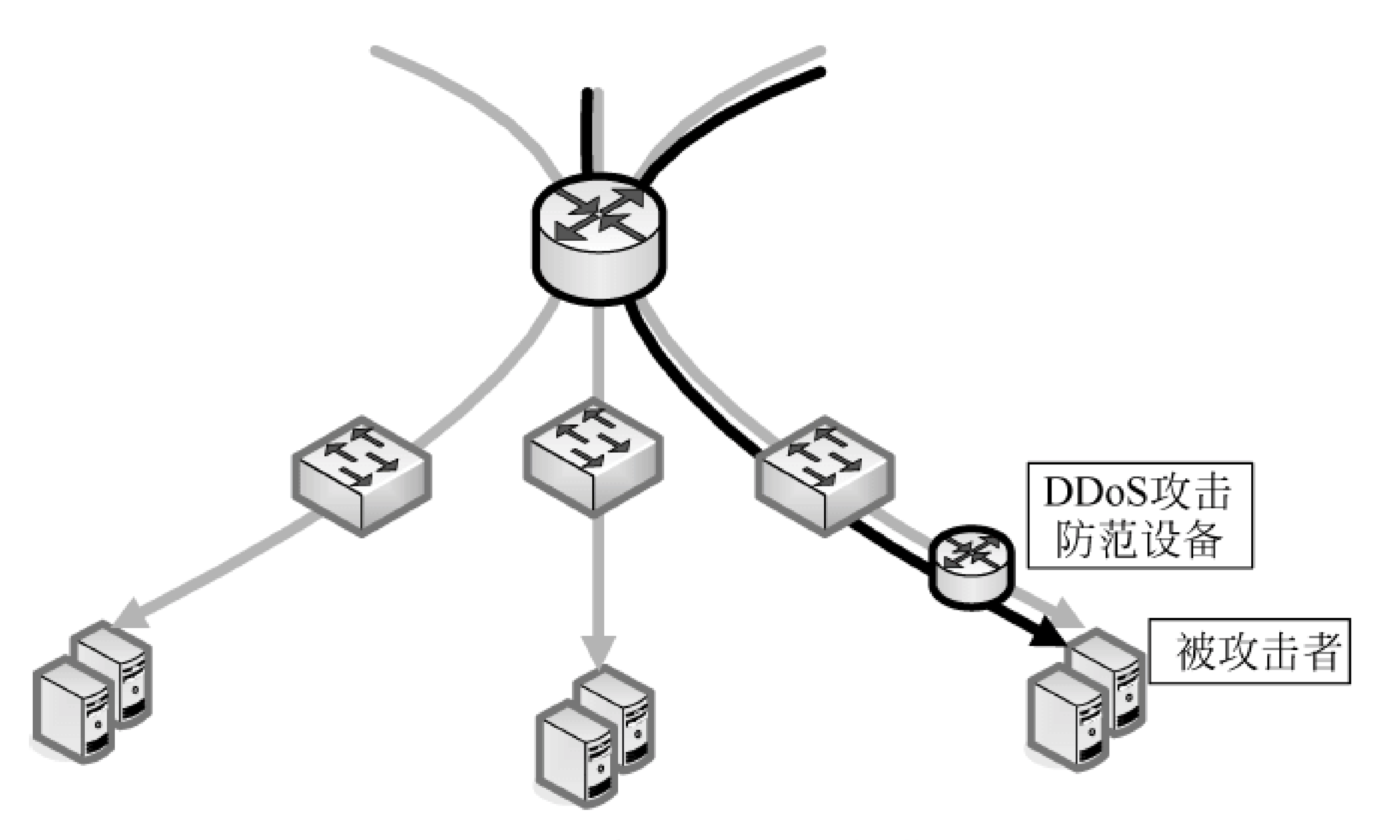


图 3-18　串行部署防御模式

此种部署模式实施起来比较简单，但有以下几个较为明显的弱点，例如，任何时候流量都经过防范设备，可能会成为性能瓶颈；在需要保护的目标设备比较多时，投资较高；对来自上游的基于带宽的 DDoS 攻击无法提供有效保护。

2）旁路部署防御 DDoS 攻击

完整的 DDoS 保护围绕以下 4 个关键主题建立：

（1）要缓解攻击，而不只是检测；

（2）从恶意业务中精确辨认出正常的业务，维持业务继续进行，而不只是检测攻击的存在；

（3）内含性能和体系结构能对上游进行配置，保护所有易受损点；

（4）维持可靠性和成本效益可升级性。

旁路式部署防御模式可以完全围绕这几个关键主题进行，没有串行模式的几大弱点，可以应用在各种网络中，对网络设备和服务器等提供保护，如图 3-19 所示。

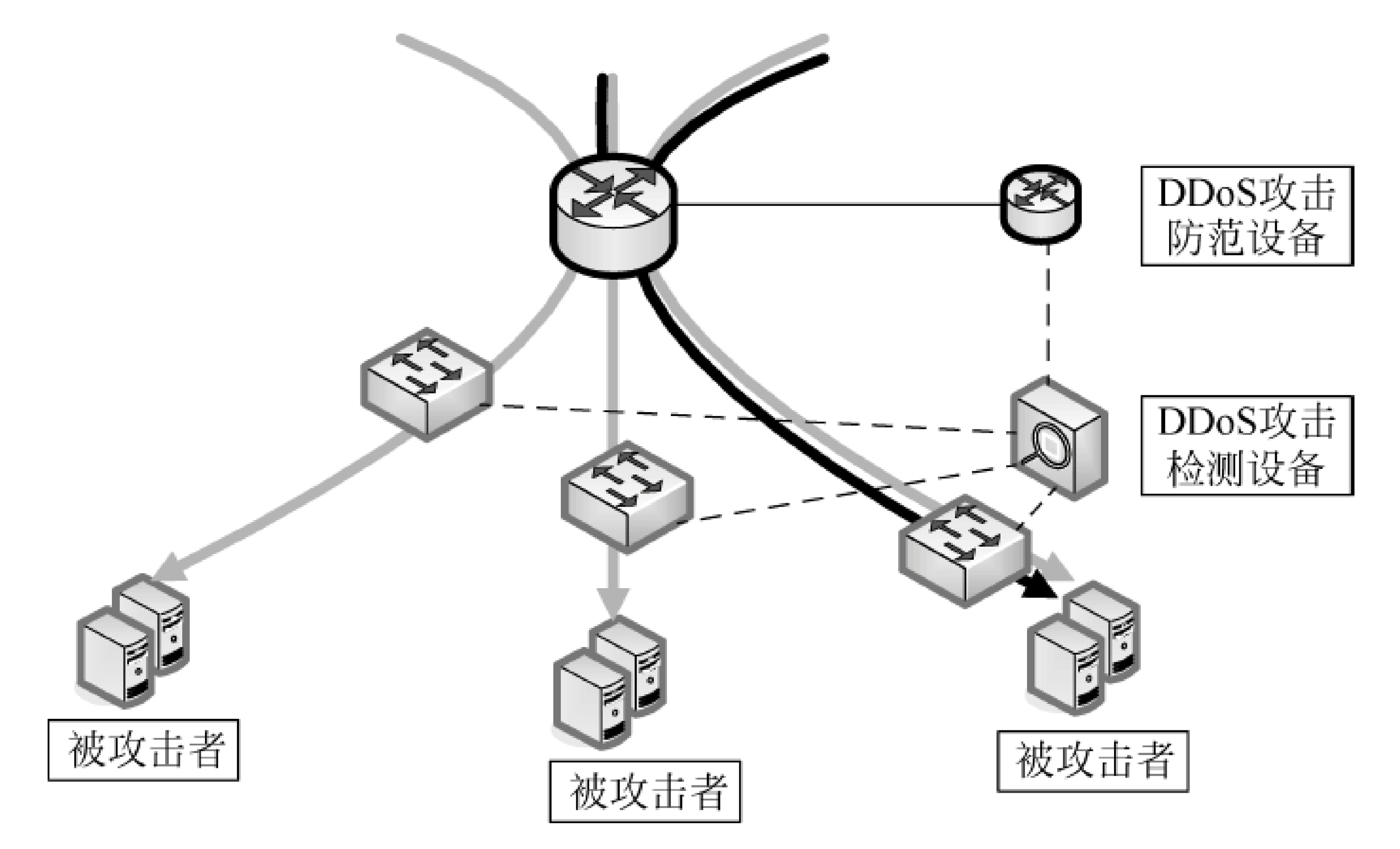


图 3-19　旁路部署防御模式

此种部署模式在原有网络的基础上实施，对原有网络没有任何改变。此方式需要 DDoS 攻击检测器和流量异常检测手段，当检测器发现 DDoS 攻击后，直接通知 DDoS 防范器将流量引导到 DDoS 防范器进行过滤，然后将过滤后正常的流量继续传送到目标地址。

这种模式在检测、转移、验证和转发的基础上实施一个完整 DDoS 保护解决方案来提供完全保护。

3.6 网络后门

简单地说，后门是攻击者再次进入网络或者是系统而不被发现的隐蔽通道。

有人说，留后门是一种艺术。留后门并不是一项简单的工作，入侵者不但要留下下次进入的通道，而且还要对自己所做的一切加以隐藏，如果建立起的后门马上就被管理员发现就没有任何用处了。所以，只要是不容易被发现的后门都是好后门。

1. 留后门的目的

(1) 保持对目标系统的长期控制；

(2) 监听目标系统的行动或记录目标系统的敏感信息，随时报告入侵者。

2. 后门的分类

留后门的方法多不胜数，可以利用不同后门的特点对后门进行分类。

按后门的整体特点可分为主动后门和被动后门。主动后门是后门程序主动监听某个端口或进程，随时等待连接，后门的特征非常明显。被动后门不会做任何工作，只有连接者去连接的时候才能表现出后门的特征。

按开放端口情况可分为开放端口的后门、不开放端口的后门、利用系统已经开放的端口的后门。

按工作模式可分为命令模式的后门、图形界面的后门、B/S 结构基于浏览器的后门。

按连接模式可分为正向连接后门、反向连接后门。

3.7 清除日志

清除日志是黑客入侵的最后的一步，黑客能做到来无影去无踪，这一步起到决定性的作用。大多数系统都是通过记录日志文件来检测是谁进入过系统并且停留了多长时间，根据日志文件所设置的级别不同，还可以发现入侵者做了些什么，对哪些文件进行了操作。

1. 清除 IIS 日志

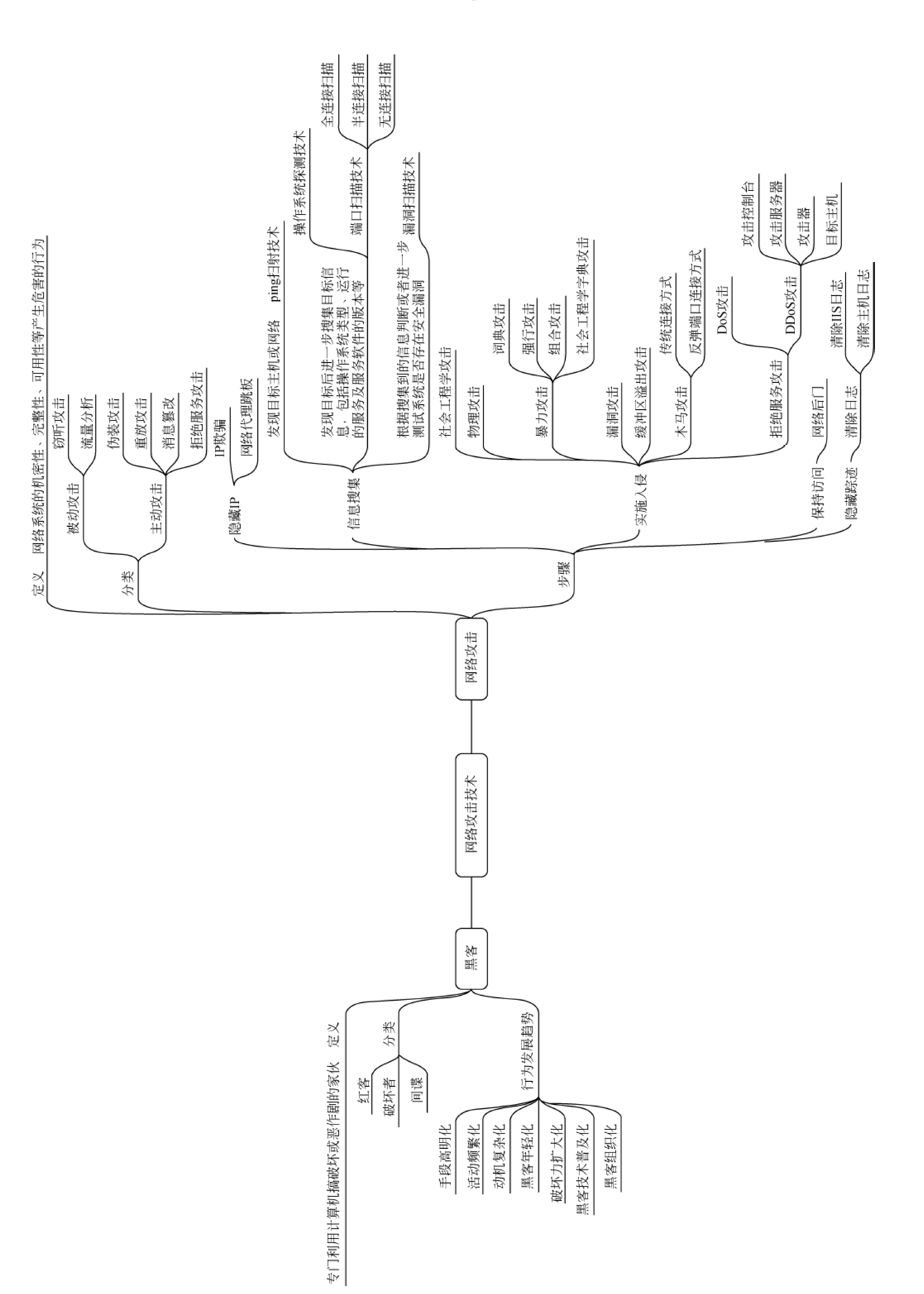
当用户访问某个 IIS 服务器后，无论是正常的访问还是非正常的访问，IIS 都会记录访问者的 IP 地址以及访问时间等信息。这些信息记录在 Winnt\System32\logFiles 目录下，打开任一文件夹下的任一文件，可以看到 IIS 日志的基本格式，记录了用户访问的服务器文件、用户登录时间、用户的 IP 地址，以及用户浏览器和操作系统的版本号。

清除 IIS 日志的最简单的方法是直接到该目录下删除这些文件夹，但是全部删除文件后，一定会引起管理员的怀疑。一般入侵的过程是短暂的，只会保存到一个 LOG 文件中，只要在该 LOG 文件中删除所有自己的记录即可。也可以使用工具软件 CleanIISLog. exe 等清除指定的 IIS 日志记录。

2. 清除主机日志

主机日志包括三类日志：应用程序日志、安全日志和系统日志。可以在计算机上通过控制面板下的管理工具下的“事件查看器”查看日志信息。当非法入侵对方的计算机后，这些日志同样会记载一些入侵者的信息，为了防止被发现，也需要清除这些日志。清除主机日志可以使用 clearlogs. exe 等工具软件实现。

3.8 本章小结


黑客
定义
专门利用计算机搞破坏或恶作剧的家伙
分类
红客
破坏者
间谍
行为发展趋势
手段高明化
活动频繁化
动机复杂化
黑客年轻化
破坏力扩大化
黑客技术普及化
黑客组织化
网络攻击技术
网络攻击
定义
网络系统的机密性、完整性、可用性等产生危害的行为
分类
被动攻击
窃听攻击
流量分析
主动攻击
伪装攻击
重放攻击
消息篡改
拒绝服务攻击
步骤
隐藏IP
IP欺骗
网络代理跳板
信息搜集
发现目标主机或网络
ping扫射技术
发现目标后进一步搜集目标信息，包括操作系统类型、运行的服务及服务软件的版本等
操作系统探测技术
端口扫描技术
全连接扫描
半连接扫描
无连接扫描
根据搜集到的信息判断或者进一步测试系统是否存在安全漏洞
漏洞扫描技术
实施入侵
社会工程学攻击
物理攻击
暴力攻击
词典攻击
强行攻击
组合攻击
社会工程学字典攻击
漏洞攻击
缓冲区溢出攻击
木马攻击
传统连接方式
反弹端口连接方式
拒绝服务攻击
DoS攻击
DDoS攻击
攻击控制台
攻击服务器
攻击器
目标主机
保持访问
网络后门
隐藏踪迹
清除日志
清除IIS日志
清除主机日志

3.9 习　　题

一、填空题

1. X.800 和 RFC 2828 对网络攻击进行了分类，分为被动攻击和主动攻击。(　　)试图获得或利用系统的信息，但不会对系统的资源造成破坏。

2. 主动攻击一般分为伪装攻击、(　　)、消息篡改和拒绝服务攻击 4 类。

3. 网络攻击五部曲包括(　　)、信息搜集、实施入侵、保持访问和隐藏踪迹。

4. (　　)是伪造某台主机的 IP 地址的技术，其实质就是让一台主机来扮演另一台主机，以达到隐藏自己的目的。

5. (　　)是依靠发送 FIN 来判断目标计算机的指定端口是否活动，也称为秘密扫描。

6. 网卡的工作模式包括广播模式、组播模式、直接模式和(　　)。

7. (　　)就是利用人们的心理特征骗取用户的信任，获取机密信息、系统设置等不公开的资料。

8. (　　)是指当计算机程序向缓冲区内填充的数据位数超过缓冲区本身的空间，溢出的数据覆盖在合法数据上。

9. 木马的连接方式包括传统连接方式和(　　)连接方式。

10. 一个比较完善的 DDoS 攻击体系分成(　　)、攻击服务器、攻击器和目标主机 4 个部分。

二、选择题

1. 在黑客攻击技术中，(　　)是黑客发现获得主机信息的一种最佳途径。

   A. 端口扫描　　B. 缓冲区溢出　　C. 网络监听　　D. 口令破解

2. 字典攻击被用于(　　)。

   A. 用户欺骗　　B. 远程登录　　C. 网络嗅探　　D. 破解密码

3. 一次字典攻击能否成功，主要决定于(　　)。

   A. 字典文件　　B. 计算机性能　　C. 网络速度　　D. 黑客经验

4. 为了防御网络监听，最常用的方法是(　　)。

   A. 采用物理传输(非网络)　　B. 信息加密

   C. 无线网　　D. 使用专线传输

5. 向有限的空间输入超长的字符串是(　　)攻击。

   A. 缓冲区溢出　　B. 网络监听　　C. 端口扫描　　D. IP 欺骗

6. 使用服务器中充斥着大量要求回复的信息，消耗带宽，导致网络或系统信息无法正常服务，这属于(　　)攻击。

   A. 拒绝服务　　B. 文件共享

   C. BIND 漏洞　　D. 远程过程调用

7. 拒绝服务攻击是对计算机网络的(　　)安全属性的破坏。

   A. 保密性　　B. 完整性

   C. 可用性　　D. 不可否认性

8. 假如你向一台远程主机发送特定的数据包，却不想远程主机响应你的数据包，这是(　　)攻击手段。

A. 缓冲区溢出　　B. 地址欺骗　　C. 拒绝服务　　D. 暴力攻击

9. 小李在使用 super scan 对网络进行扫描时发现，某一个主机开放了 25 和 110 端口，此主机最有可能是(　　)。

A. 文件服务器　　B. 邮件服务器　　C. Web 服务器　　D. DNS 服务器

10. 在 DDoS 攻击中，通过非法入侵并被控制，但并不向被攻击者直接发起攻击的计算机称为(　　)。

A. 攻击控制台　　B. 攻击服务器　　C. 攻击器　　D. 目标主机

11. 对利用软件缺陷进行的网络攻击，最有效的防范方法是(　　)。

A. 及时更新补丁程序　　B. 安装防病毒软件

C. 安装防火墙　　D. 安装漏洞扫描软件

12. 缓冲区溢出的最大危害是(　　)。

A. 使系统崩溃　　B. 使系统运行出错

C. 管理员权限下运行黑客程序　　D. 侵占其他用户内存

13. (　　)不是以破坏信息可用性为目的的攻击行为。

A. Ping of Death　　B. SYN 泛洪　　C. 安装后门程序　　D. DDoS

14. 端口扫描技术(　　)。

A. 只能作为攻击工具

B. 只能作为防御工具

C. 只能作为检查系统漏洞的工具

D. 既可以作为攻击工具，也可以作为防御工具

15. 采用模拟攻击漏洞探测技术的好处是(　　)。

A. 可以探测到所有漏洞　　B. 完全没有破坏性

C. 对目标系统没有负面影响　　D. 探测结果准确率高

16. 半连接端口扫描技术显著的特点是(　　)。

A. 不需要特殊权限

B. 不会在日志中留下任何记录

C. 不建立完整的 TCP 连接

D. 可以扫描到 UDP 端口

17. 以下对 DoS 攻击的描述，正确的是(　　)。

A. 不需要侵入受攻击的系统

B. 以窃取目标系统上的机密信息为目的

C. 导致目标系统无法正常处理用户的请求

D. 若目标系统没有漏洞，远程攻击不会成功

18. Windows 系统能设置在几次无效登录后锁定账号，可以防止(　　)。

A. 木马　　B. 暴力破解　　C. IP 欺骗　　D. 缓冲区溢出

19. TCP SYN 泛洪攻击的原理是利用了(　　)。

A. TCP 三次握手过程　　B. TCP 面向流的工作机制

C. TCP数据传输中的窗口技术　　D. TCP连接终止时的FIN报文

20. 木马与病毒的最大区别是(　　)。

A. 木马不破坏文件,而病毒会破坏文件

B. 木马无法自我复制,而病毒能够自我复制

C. 木马无法使数据丢失,而病毒会使数据丢失

D. 木马不具有潜伏性,而病毒有潜伏性

21. 木马无法通过(　　)隐藏自己。

A. 任务栏　　B. 任务管理器

C. 邮件服务器　　D. 修改系统配置文件

22. 计算机感染木马后的典型现象是(　　)。

A. 程序异常退出　　B. 有未知程序试图建立网络连接

C. 邮箱被垃圾邮件填满　　D. Windows系统黑屏

23. SYN泛洪攻击利用(　　)。

A. 操作系统漏洞　　B. 通信协议缺陷

C. 缓冲区溢出　　D. 用户警惕性不够

24. 以下(　　)不属于防止口令猜测的措施。

A. 严格限定从一个给定的终端进行非法认证的次数

B. 确保口令不在终端上再现

C. 防止用户使用太短的口令

D. 使用机器产生的口令

25. (　　)不是以破坏信息保密性为目的的攻击行为。

A. 信息嗅探　　B. 信息截获

C. 安装后门程序　　D. DDoS

26. 属于操作系统中日志记录功能的是(　　)。

A. 控制用户的作业排序和运行

B. 以合理的方式处理错误事件,而不至于影响其他程序的正常运行

C. 保护系统程序和作业,禁止不合要求的对程序和数据的访问

D. 对计算机用户访问系统和资源的情况进行记录

27. (　　)不是黑客发现主机系统漏洞的步骤。

A. 通过主机扫描发现在线主机

B. 通过端口扫描发现开启的服务

C. 通过主动探测获得操作系统类型和版本号

D. 骗取用户口令

28. (　　)是最主要的主机系统漏洞。

A. 缓冲区溢出　　B. Unicode漏洞

C. Ping of Death　　D. Land

29. (　　)不是对主机系统实施的拒绝服务攻击。

A. Ping of Death　　B. SYN泛洪

C. Smurf　　D. 穷举法猜测用户登录口令

30. (　　)无法破坏网络的可用性。

A. 病毒　　B. 拒绝服务攻击

C. 非法访问　　D. 线缆遭受破坏

31. (　　)和信息保密性无关。

A. 加密/解密算法　　B. 终端接入控制

C. 病毒　　D. 拒绝服务攻击

32. (　　)不属于主动攻击。

A. 流量分析　　B. 重放　　C. IP 地址欺骗　　D. 拒绝服务

33. (　　)属于主动攻击。

A. 篡改和破坏数据　　B. 嗅探数据　　C. 数据流分析　　D. 非法访问

34. 关于 MAC 表溢出攻击,以下选项中描述错误的是(　　)。

A. MAC 表能够存储的转发项是有限的

B. 交换机无法鉴别 MAC 帧的源 MAC 地址和接收端口之间的绑定关系

C. 交换机广播没有转发项与之匹配的 MAC 帧

D. 不允许存在多项 MAC 地址不同但转发端口相同的转发项

35. 关于 MAC 地址欺骗攻击,以下选项中描述错误的是(　　)。

A. 交换机无法鉴别 MAC 帧的源 MAC 地址和接收端口之间的绑定关系

B. 交换机根据最新的 MAC 帧的源 MAC 地址和接收端口之间的绑定关系更新转发项

C. 终端可以伪造自己的 MAC 地址

D. 允许存在多项 MAC 地址相同但转发端口不同的转发项

36. 关于 ARP 欺骗攻击,以下选项中描述正确的是(　　)。

A. 广播的 ARP 请求报文中给出黑客终端的 MAC 地址与攻击目标的 IP 地址之间的绑定关系

B. 广播的 ARP 请求报文中给出攻击目标的 MAC 地址与黑客终端的 IP 地址之间的绑定关系

C. 广播的 ARP 请求报文中给出黑客终端的 MAC 地址与黑客终端的 IP 地址之间的绑定关系

D. 广播的 ARP 请求报告中给出攻击目标的 MAC 地址与攻击目标的 IP 地址之间的绑定关系

37. 关于 SYN 泛洪攻击,以下选项中描述错误的是(　　)。

A. TCP 会话表中的连接项是有限的

B. 未完成建立过程的 TCP 连接占用连接项

C. 用伪造的、网络中本不存在的 IP 地址发起 TCP 连接建立过程

D. 未完成建立过程的 TCP 连接永久占用连接项

38. 关于 Smurf 攻击,以下选项中描述错误的是(　　)。

A. 封装 ICMP ECHO 请求报文的 IP 分组的源 IP 地址是攻击目标的 IP 地址

B. 封装 ICMP ECHO 请求报文的 IP 分组的目的 IP 地址是广播地址

C. 接收 ICMP ECHO 请求报文的终端回送 ICMP ECHO 响应报文

D. 单个 ICMP ECHO 请求报文只能引发单个 ICMP ECHO 响应报文

39. 关于间接 DDoS 攻击,以下选项中描述错误的是(　　)。
A. 傀儡机随机生成有效 IP 地址集
B. 正常主机系统发送对应的响应报文
C. 正常主机系统不对接收到的请求报文进行源端鉴别
D. 傀儡机发送的请求报文以随机生成的有效 IP 地址为源 IP 地址

40. 以下关于网络钓鱼的说法中,不正确的是(　　)。
A. 网络钓鱼融合了伪装、欺骗等多种攻击方式
B. 网络钓鱼与 Web 服务没有关系
C. 典型的网络钓鱼攻击是将被攻击者引诱到一个精心设计的钓鱼网站上
D. 网络钓鱼是“社会工程攻击”的一种形式

41. 关于钓鱼网站,以下选项中描述错误的是(　　)。
A. 黑客构建模仿某个著名网站的假网站
B. 假网站的 IP 地址与著名网站的 IP 地址相同
C. 正确的域名得到错误的解析结果
D. 用户不对访问的网站的身份进行鉴别

42. 利用 ICMP 进行扫描时,(　　)是可以扫描的目标主机信息。
A. IP 地址　　B. 操作系统版本　　C. 漏洞　　D. 弱口令

43. 关于黑客入侵,以下选项中描述错误的是(　　)。
A. 存在黑客终端与攻击目标之间的传输路径
B. 攻击目标存在漏洞
C. 黑客通过扫描发现攻击目标存在的漏洞
D. 黑客必须已经获取攻击目标的管理员账户信息

44. (　　)攻击与操作系统漏洞无关。
A. 非法登录主机系统
B. 向主机系统植入病毒
C. 缓冲区溢出
D. 消耗掉主机系统连接网络的链路的带宽

45. (　　)不是 ARP 欺骗攻击的技术原理。
A. 终端接收到 ARP 报文,记录 ARP 报文中的 IP 地址与 MAC 地址对
B. 如果 ARP 缓冲区中已经存在 IP 地址与 MAC 地址对,以该 MAC 地址作为该 IP 地址的解析结果
C. 可以在 ARP 报文中伪造 IP 地址与 MAC 地址对
D. ARP 缓存区中的 IP 地址与 MAC 地址对存在寿命

三、判断题

1. TCP SYN 泛洪攻击属于一种典型的 DoS 攻击。
2. 木马有时称为木马病毒,但却不具有计算机病毒的主要特征。
3. 要实现 DDoS 攻击,攻击者必须能够控制大量的计算机为其服务。
4. 在 LAND 攻击中,LAND 攻击报文的源 IP 地址和目的 IP 地址是相同的。

5. 拒绝服务攻击就是利用更多的傀儡机对目标发起进攻，使目标系统资源耗尽无法处理正常用户的请求。

四、简答题

1. 黑客攻击5个步骤是什么？

2. DDoS攻击由哪4部分组成？

3. 端口扫描的基本原理是什么？

4. 什么是计算机网络安全漏洞？

5. 什么是DoS?

6. 什么是字典攻击？

7. 什么是Unicode漏洞？

8. 简述网络扫描的步骤。

五、综合题

1. 阅读下面程序，回答问题(1)～(2)。

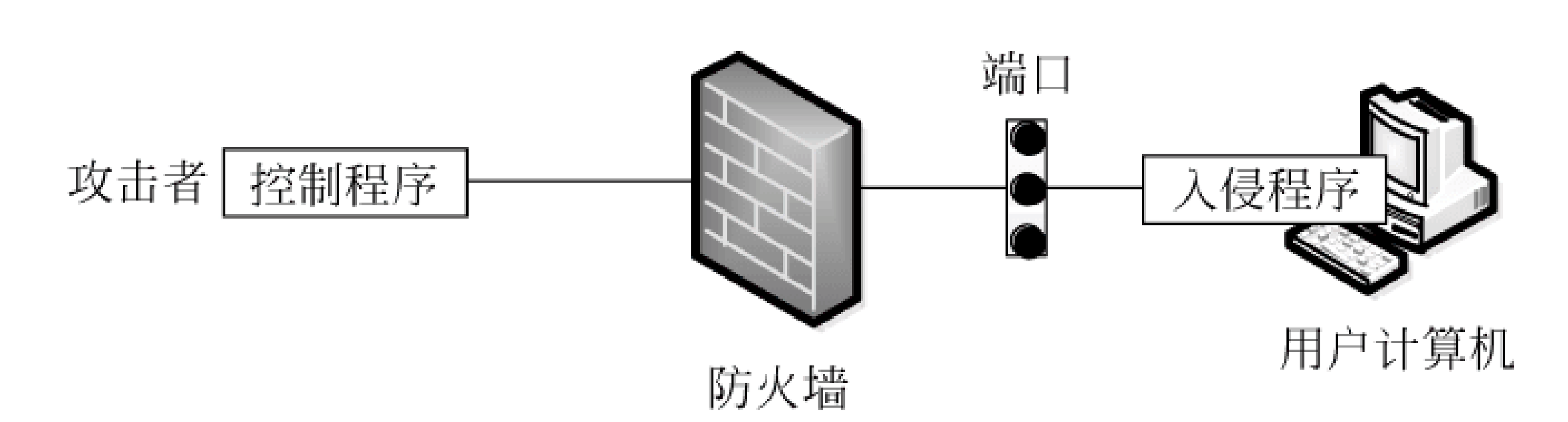
```
void function(char * str)
{
  char buffer[16];
  strcopy(buffer,str);
}
void main()
{
  int t;
  char buffer[128];
  for(i = 0;i < 127;i++)
      buffer[i] = 'A';
      buffer[127] = 0;
  function(buffer);
  print("This is a test\n");
}
```

(1) 上述代码存在什么类型的安全隐患？

(2) 造成上述隐患的两个原因是什么？

2. 阅读以下说明，回答问题(1)～(4)。

说明：特洛伊木马是一种基于客户机/服务器模式的远程控制程序，黑客可以利用木马程序入侵用户的计算机系统。木马的工作模式如下图所示。



(1) 对于传统的木马程序，侵入被攻击主机的入侵程序属于__①__。攻击者一旦获取入侵程序的__②__，便与它连接起来。

① A. 客户程序　　B. 服务器程序　　C. 代理程序　　D. 系统程序

② A. 用户名和口令　　　　　　　　B. 密钥
C. 访问权限　　　　　　　　　　D. 地址和端口号

（2）以下＿③＿和＿④＿属于计算机感染特洛伊木马后的典型现象。

③、④ A. 程序堆栈溢出　　　　　　B. 有未知程序试图建立网络连接
C. 邮箱被莫名邮件填满　　　　　D. 系统中有可疑的进程在运行

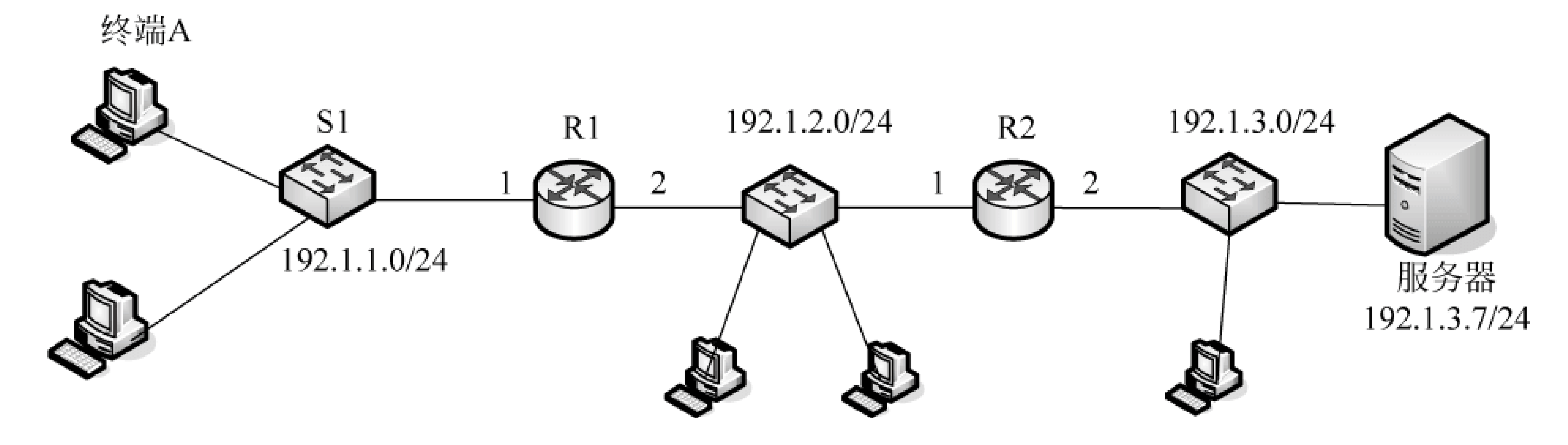
（3）安装了防火墙软件的主机可以利用防火墙的＿⑤＿功能，有效地防止外部非法连接来拦截木马。

⑤ A. 身份认证　　B. 地址转换　　C. 日志记录　　D. 包过滤

（4）以下措施中能有效防治木马入侵的有＿⑥＿和＿⑦＿。

⑥、⑦ A. 不随意下载来历不明的软件　　B. 仅开放非系统端口
C. 实行加密数据传输　　　　　　D. 实行实时网络连接监控程序

3. 网络结构如下图所示，回答以下问题。



（1）如果终端 A 想要通过 Smurf 攻击服务器，给出终端 A 发送的三种类型的 ICMP ECHO 请求报文的源 IP 和目的 IP。

（2）如果要求网络能够阻止终端 A 发起对服务器的 Smurf 攻击，给出在交换机 S1、路由器 R1 和路由器 R2 上采取的措施。

第 4 章 计算机病毒

【本章学习目标】

- 理解计算机病毒定义
- 了解计算机病毒的起源与发展
- 掌握计算机病毒的命名方式
- 了解计算机病毒的分类和特征
- 掌握计算机病毒技术
- 掌握计算机病毒的检测与防范方法

4.1 计算机病毒概述

4.1.1 计算机病毒的定义及发展

1. 计算机病毒定义

计算机病毒(Computer Virus)在《中华人民共和国计算机信息系统安全保护条例》中被明确定义,病毒指“编制者在计算机程序中插入的破坏计算机功能或者破坏数据,影响计算机使用并且能够自我复制的一组计算机指令或者程序代码”。

可以从下面几个方面来理解计算机病毒的定义。首先,病毒是通过磁盘或网络等媒介传播扩散且能“传染”其他程序的程序。其次,病毒能够实现自我复制且借助一定的载体存在,具有潜伏性、传染性和破坏性。再次,病毒是一种人为制造的程序,它不会自然产生,是精通编程的人精心编制的,通过不同的途径寄生在存储介质中,当条件成熟时,就会复制、传播,甚至变异后传播,使计算机的资源受到不同程度的破坏。

2. 计算机病毒的发展

随着计算机及其网络技术的快速发展,计算机病毒日趋复杂多变,其破坏能力和传播能力也不断增强。计算机病毒的发展主要经历了 5 个重要阶段。

1) 原始病毒阶段(第一阶段)

1986—1989 年,计算机应用程序较少,大部分为单机运行,计算机病毒的种类也比较少,且难以广泛传播,清除病毒也相对容易。这一阶段病毒的主要特点为:攻击目标和破坏性比较单一,主要通过截获系统中断向量的方式监视系统的运行状态,并在一定的条件下对目标进行传染,病毒程序不具有自我保护功能,较容易被人们分析、识别和清除。

2) 混合型病毒阶段(第二阶段)

1989—1991 年,是计算机病毒由简到繁的发展阶段。随着计算机局域网的应用和普

及，计算机病毒达到了第一次流行高峰。这一阶段病毒的主要特点为：攻击目标趋于混合，以更为隐蔽的方法驻留在内存和传染目标中，系统感染病毒后没有明显的特征，病毒程序具有自我保护功能，出现众多病毒的变种。

3）多态型病毒阶段（第三阶段）

1992年—20世纪90年代中期，病毒的主要特点为：在每次传染目标时，放入宿主程序中的病毒程序大部分都是可变的，因此防病毒软件查杀非常困难。如1994年在国内出现的“幽灵”病毒。在此阶段，病毒技术开始向多维化方向发展。

4）网络病毒阶段（第四阶段）

从20世纪90年代后期开始，随着国际互联网的广泛发展，依赖互联网络传播的邮件病毒和宏病毒等大肆泛滥，病毒呈现出传播快、隐蔽性强、破坏性大的特点。从这一阶段开始，防病毒产业开始产生并逐步成为规模较大的新兴产业。

5）主动攻击型病毒阶段（第五阶段）

近几年，典型病毒的代表为“冲击波”病毒、“勒索”病毒和木马等。各种病毒具有主动攻击性，利用操作系统的漏洞进行攻击性的传播扩散，并不需要任何物理媒介或操作，用户只要接入互联网就有可能被感染，病毒对网络系统软硬件和重要信息的危害性更大。

3. 计算机病毒的命名方式

为了进行防范和研究防病毒技术，需要规范计算机病毒的命名方式。通常综合病毒的特征和对用户造成的影响等多方面情况，由防病毒厂商给出一个合适名称。目前，公安部门也正在规范病毒的命名。病毒的命名并无统一的规定，不同防病毒厂商的命名规则也不尽一致，基本上是采用前后缀法来进行命名。命名由多个前缀与后缀组合，中间以点“.”分隔，一般格式为：[前缀].[病毒名].[后缀]。如震荡波蠕虫病毒的变种为Worm.Sasser.c，其中Worm指病毒的种类为蠕虫，Sasser是病毒名，c指该病毒的变种。

1）病毒前缀

病毒前缀表示一个病毒的种类，如木马病毒的前缀是Trojan，蠕虫病毒的前缀为Worm，宏病毒的前缀是Macro，后门病毒的前缀是Backdoor，脚本病毒的前缀是Script，系统病毒的前缀是Win32、PE、W32等，捆绑机病毒的前缀是Binder，玩笑病毒的前缀是Joke。

2）病毒名

病毒名即病毒的名称，如“病毒之母”CIH病毒及其变种的名称一律为CIH，冲击波病毒名为Blaster。病毒名也有一些约定俗成的方式，可按病毒发作的时间命名，如黑色星期五病毒；也可按病毒发作症状命名，如小球病毒；或按病毒自身包含的标志命名，如CIH病毒；还可按病毒发现地命名，如耶路撒冷病毒；或按病毒的字节长度命名，如1575病毒。

3）病毒后缀

病毒后缀表示一个病毒的变种特征，一般是采用英文中的26个字母来表示。如Worm.Sasser.c是指震荡波蠕虫病毒的变种c。如果病毒的变种太多，也可采用数字和字母混合的方式来表示。

4.1.2 计算机病毒分类

通常，计算机病毒可按如下方式进行分类。

1. 按寄生方式分类

（1）引导型病毒。引导型病毒是指寄生在磁盘引导区或主引导区的计算机病毒。此种病毒利用系统引导时，不对主引导区的内容正确与否进行判别的缺点，在引导系统的过程中侵入系统，驻留内存，监视系统运行，伺机传染和破坏。按照引导型病毒在硬盘上的寄生位置又可细分为主引导记录病毒和分区引导记录病毒。主引导记录病毒感染硬盘的主引导区，如大麻病毒、2708 病毒、火炬病毒等；分区引导记录病毒感染硬盘的活动分区引导记录，如小球病毒、Girl 病毒等。

（2）文件型病毒。文件型病毒是指能够寄生在文件中的计算机病毒。这类病毒程序感染可执行文件或数据文件。如 1575/1591 病毒、848 病毒感染 COM 和 EXE 等可执行文件；Macro/Concept、Macro/Atoms 等宏病毒感染 DOC 文件。

（3）复合型病毒。复合型病毒是指同时具有引导型病毒和文件型病毒寄生方式的计算机病毒。这种病毒扩大了病毒程序的传染途径，它既感染磁盘的引导记录，又感染可执行文件。当染有此种病毒的磁盘用于引导系统或调用执行染毒文件时，病毒会被激活。因此在检测、清除复合型病毒时，必须全面彻底地根治。如果只发现该病毒的一个特性，把它只当作引导型或文件型病毒进行清除，虽然表面上是清除了，但还留有隐患，这种经过消毒后的“洁净”系统更赋有攻击性。这种病毒有 Flip 病毒、新世际病毒、One-half 病毒等。

2. 按破坏性分类

（1）良性病毒。良性病毒是指那些只是为了展示自己，并不彻底破坏系统和数据，但会大量占用 CPU 时间，增加系统开销，降低系统工作效率的一类计算机病毒。这种病毒多数是恶作剧者的产物，他们的目的不是为了破坏系统和数据，而是为了让使用染毒计算机的用户通过显示器或扬声器看到或听到病毒设计者的编程技术。这类病毒有小球病毒、1575/1591 病毒、救护车病毒、女鬼病毒、Dabi 病毒等。

（2）恶性病毒。恶性病毒是指那些一旦发作后，就会破坏系统或数据，造成计算机系统瘫痪的一类计算机病毒。这类病毒有黑色星期五病毒、火炬病毒、米开朗基罗病毒等。这种病毒危害性极大，有些病毒发作后可能给用户造成不可挽回的损失。

3. 按入侵方式分类

（1）源代码嵌入攻击型。这类病毒入侵的主要是高级语言的源程序，病毒在源程序编译之前插入病毒代码，最后随源程序一起被编译成可执行文件，这样刚生成的文件就是带毒文件。

（2）代码取代攻击型。这类病毒主要用它自身的病毒代码取代某个入侵程序的整个或部分模块，这类病毒比较少见，它主要攻击特定的程序，针对性较强，但是不易被发现，清除起来比较困难。

（3）系统修改型。这类病毒主要是通过自身程序覆盖或修改系统中的某些文件来达到调用或替代操作系统中的部分功能，由于是直接感染系统，危害较大，是最为多见的一种病毒类型，多为文件型病毒。

（4）外壳附加型。这类病毒通常被附加在正常程序的头部或尾部，相当于给程序添加了一个外壳，在被感染的程序执行时，病毒代码先被执行，然后才将正常程序调入内存。

4.1.3 计算机病毒的主要特征

要防范计算机病毒，首先需要了解计算机病毒的特征和破坏机理，为防范和清除计算机病毒提供真实可靠的依据。根据对计算机病毒的产生、传染和破坏行为的分析，计算机病毒一般具有以下特征：非授权可执行性、隐蔽性、传染性、潜伏性、破坏性（表现性）和可触发性。

1. 非授权可执行性

用户在调用执行一个程序时，通常把系统控制权交给这个程序，并分配给它相应的系统资源，如内存，从而使之能够运行完成用户的需求，因此程序执行的过程对用户是透明的。正常用户不会明知是病毒程序，而故意调用执行。计算机病毒虽然是非法程序，但具有正常程序的一切特性，如可存储性、可执行性。它隐藏在合法的程序或数据中，当用户运行正常程序时，病毒伺机窃取到系统的控制权，得以抢先运行，然而此时用户还认为是在执行正常程序。

2. 隐蔽性

计算机病毒是一种编程技巧高超、短小精悍的可执行程序。它通常粘附在正常程序中或磁盘引导扇区中，或者磁盘上标为坏簇的扇区中，以及一些空闲概率较大的扇区中，这是它的非法可存储性。病毒想方设法隐藏自身，就是为了防止用户察觉。

3. 传染性

计算机病毒不但自身具有破坏性，更有害的是具有传染性，一旦病毒被复制或产生变种，其发展速度之快令人难以预防。传染性是病毒的基本特征。在生物界，病毒通过传染从一个生物体扩散到另一个生物体。在适当的条件下，它可得到大量繁殖，并使被感染的生物体表现出病症甚至死亡。同样，计算机病毒也会通过各种渠道从已被感染的计算机扩散到未被感染的计算机，在某些情况下造成被感染的计算机工作失常甚至瘫痪。与生物病毒不同的是，计算机病毒是一段人为编制的计算机程序代码，这段程序代码一旦进入计算机并得以执行，它就会搜寻其他符合其传染条件的程序或存储介质，确定目标后再将自身代码插入其中，达到自我繁殖的目的。只要一台计算机染毒，如不及时处理，病毒会在这台计算机上迅速扩散，通过各种可能的渠道，如 U 盘、计算机网络去传染其他的计算机。当在一台计算机上发现病毒时，往往曾在这台计算机上用过的 U 盘已被感染病毒，而与这台计算机联网的其他计算机也许也被该病毒传染上了。是否具有传染性是判别一个程序是否为计算机病毒的最重要条件。病毒程序通过修改磁盘扇区信息或文件内容并把自身嵌入到其中以达到病毒的传染和扩散。

4. 潜伏性

计算机病毒具有依附于其他媒体而寄生的能力，这种媒体我们称为计算机病毒的宿主。依靠病毒的寄生能力，病毒传染合法的程序和系统后，不立即发作，而是悄悄隐藏起来，然后在用户未察觉的情况下进行传染。因此，病毒的潜伏性越好，它在系统中存在的时间就越长，病毒传染的范围也越广，其危害性也越大。

5. 破坏性（表现性）

无论何种病毒程序一旦侵入系统都会对操作系统的运行造成不同程度的影响。即使不直接产生破坏作用的病毒程序也要占用系统资源（如占用内存空间，占用磁盘存储空间以及

系统运行时间等)。而绝大多数病毒程序要显示一些文字或图像,影响系统的正常运行,还有一些病毒程序删除文件,加密磁盘中的数据,甚至摧毁整个系统和数据,使之无法恢复,造成无可挽回的损失。因此,病毒程序的负面作用体现在轻者降低系统工作效率,重者导致系统崩溃、数据丢失。病毒程序的破坏性或表现性体现了病毒设计者的真正意图。

6. 可触发性

计算机病毒一般都有一个或者几个触发条件。满足其触发条件可以激活病毒的传染机制,使之进行传染,或者激活病毒的表现部分或破坏部分。触发的实质是一种条件的控制,病毒程序可以依据设计者的要求,在一定条件下实施攻击。这个条件可以是敲入特定字符,使用特定文件,某个特定日期或特定时刻,或者是病毒内置的计数器达到一定次数等。

4.2 计算机病毒的结构与危害

4.2.1 计算机病毒的结构

计算机病毒种类很多,但其结构一般由三部分构成,即引导模块、传播模块和表现模块。

1. 引导模块

引导模块的功能是将病毒加载到内存中,并对其存储空间进行保护,以防被其他程序所覆盖,同时修改一些中断及高端内存,保存原中断向量等系统参数,为传播做准备。它也称为潜伏机制模块,具有初始化、隐藏和捕捉功能。引导模块随着感染的宿主程序的运行进入内存,先初始化运行环境,为传染机制做好准备;然后,利用各种隐藏方式躲避检测,欺骗系统;最后,不断捕捉感染目标交给传播模块。

2. 传播模块

传播模块是病毒程序的核心,其主要功能是传播病毒,一般由两部分构成,传播条件判断部分和传播部分。前者的功能是判断计算机系统是否达到病毒传播的条件,不同病毒的传播条件不同。后者的功能是在满足传播条件时,实施具体的病毒传播,按照制定的传播方式将病毒程序嵌入到传播目标中。

3. 表现模块

表现模块由两部分构成:一是病毒的触发条件判断部分,二是病毒的具体表现部分。当判断触发条件满足时,就会调用病毒的具体表现部分,对计算机系统进行干扰和破坏。表现部分在不同病毒程序中的具体破坏和影响不同。

4.2.2 计算机病毒的危害

计算机病毒,既然称之为病毒,自然对计算机用户具有一定的危害,这种危害通常表现在以下 7 个方面。

1. 破坏数据

大部分病毒在激发时会直接破坏计算机的重要信息数据,其所利用的手段有格式化磁盘、改写文件分配表和目录区、删除重要文件或者用无意义的“垃圾”数据改写文件、破坏 CMOS 设置等。

2. 占用磁盘空间

寄生在磁盘上的病毒总要非法占用一部分磁盘空间。引导型病毒一般的侵占方式是由

病毒本身占据磁盘引导扇区，而把原来的引导区转移到其他扇区，即引导型病毒要覆盖一个磁盘扇区。被覆盖的扇区数据永久性丢失，无法恢复。文件型病毒利用一些 DOS 功能进行传染，这些 DOS 功能能够检测出磁盘的未用空间，把病毒的传染部分写到磁盘的未用空间去。所以在传染过程中一般不破坏磁盘上的原有数据，但非法侵占了磁盘空间，一些文件型病毒传染速度很快，在短时间内感染大量文件，每个文件都不同程度地加长了，就造成磁盘空间的严重浪费。

3. 抢占系统资源

除 Vienna、Casper 等少数病毒外，其他大多数病毒在动态下都是常驻内存的，这就必然抢占一部分系统资源。病毒所占用的基本内存长度大致与病毒本身长度相当，病毒抢占内存，导致内存减少，一部分软件不能运行。另外，病毒还抢占中断，干扰系统运行。

4. 影响计算机运行速度

病毒进驻内存后不但干扰系统运行，还影响计算机速度。有些病毒为了保护自己，不但对磁盘上的静态病毒加密，而且进驻内存后的动态病毒也处在加密状态。CPU 每次寻址到病毒处时要运行一段解密程序把加密的病毒解密成合法的 CPU 指令再执行；而病毒运行结束时再用一段程序对病毒重新加密。这样 CPU 需额外执行数千条以至上万条指令。

5. 病毒错误导致危害

计算机病毒与其他计算机软件的一大差别是病毒的无责任性。编制一个完善的计算机软件需要耗费大量的人力、物力，经过长时间调试完善，软件才能推出。但在病毒编制者看来既没有必要这样做，也不可能这样做。很多计算机病毒都是个别人在一台计算机上匆匆编制调试后就向外抛出的。反病毒专家在分析大量病毒后发现绝大部分病毒都存在不同程度的错误，错误病毒的另一个主要来源是变种病毒。有些初学编程者尚不具备独立编制软件的能力，出于好奇或其他原因修改别人的病毒，造成错误。计算机病毒错误所产生的后果往往是不可预见的，反病毒工作者曾经详细指出黑色星期五病毒存在 9 处错误，乒乓病毒有 5 处错误等。

6. 计算机病毒的兼容性影响系统运行

兼容性是计算机软件的一项重要指标，兼容性好的软件可以在各种计算机环境下运行，反之兼容性差的软件则对运行条件有具体要求，要求机型和操作系统版本等。病毒的编制者一般不会在各种计算机环境下对病毒进行测试，因此病毒的兼容性较差，常常导致死机。

7. 计算机病毒给用户造成严重的心理压力

据有关计算机销售部门统计，用户怀疑计算机有病毒而提出咨询约占售后服务工作量的 60％以上。经检测确实存在病毒的约占 70％，另有 30％的情况只是用户怀疑，而实际上计算机并没有感染病毒。那么用户怀疑病毒的理由是什么呢？多半是出现诸如计算机死机、软件运行异常等现象。这些现象确实很有可能是计算机病毒造成的，但又不一定是病毒引起的，实际上计算机工作异常的时候很难要求一位普通用户去准确判断是否是病毒所为。大多数用户对病毒采取宁可信其有的态度，这对于保护计算机安全无疑是十分必要的，然而往往要付出时间、金钱等方面的代价。仅仅怀疑病毒而冒然格式化磁盘所带来的损失更是难以弥补。不仅是个人单机用户，在一些大型网络系统中也难免为甄别病毒而停机。总之计算机病毒像“幽灵”一样笼罩在广大计算机用户心头，给人们造成巨大的心理压力，极大地影响了现代计算机的使用效率，由此带来的经济损失是难以估量的。

4.3 计算机病毒技术

随着软件技术的发展,计算机病毒所使用的技术也越来越复杂化。黑客们不断研究最新的计算机技术,不断尝试把新技术用于病毒,例如寄生技术、驻留技术、加密变形技术、隐藏技术等。

4.3.1 寄生技术

病毒寄生技术是文件型病毒最常用的传染方法。病毒在感染的时候,将病毒代码加入正常程序之中,原正常程序功能的全部或者部分被保留。根据病毒代码加入方式的不同,病毒寄生技术可以分为头寄生、尾寄生、插入寄生和空洞利用 4 种。前三种是源病毒代码插入宿主程序位置的不同;而空洞利用的原理是 Windows 可执行文件的结构非常复杂,里面会有很多没有使用的部分,一般是空的段或者每个段的最后部分。病毒寻找到这些没有使用的部分,然后将病毒代码分散到其中,因为被感染文件的大小没有发生变化,这样就实现了令人难以觉察的感染。著名的 CIH 病毒就是使用了空洞利用寄生技术。当然,PE 格式的修改是很困难的,一点小的错误就将使宿主程序不能运行。

1. 头寄生

实现将病毒代码放到程序的头上有两种方法:一种是将原来程序的前面一部分拷贝到程序的最后,然后将文件头用病毒代码覆盖;另一种是生成一个新的文件,首先在头的位置写上病毒代码,然后将原来的可执行文件放在病毒代码的后面,再用新的文件替换原来的文件。

使用头寄生方式的病毒基本上感染的是批处理文件和 COM 文件,因为这些文件在运行的时候不需要重新定位,所以可以任意调换代码的位置而不发生错误。头寄生的方式如图 4-1 所示。

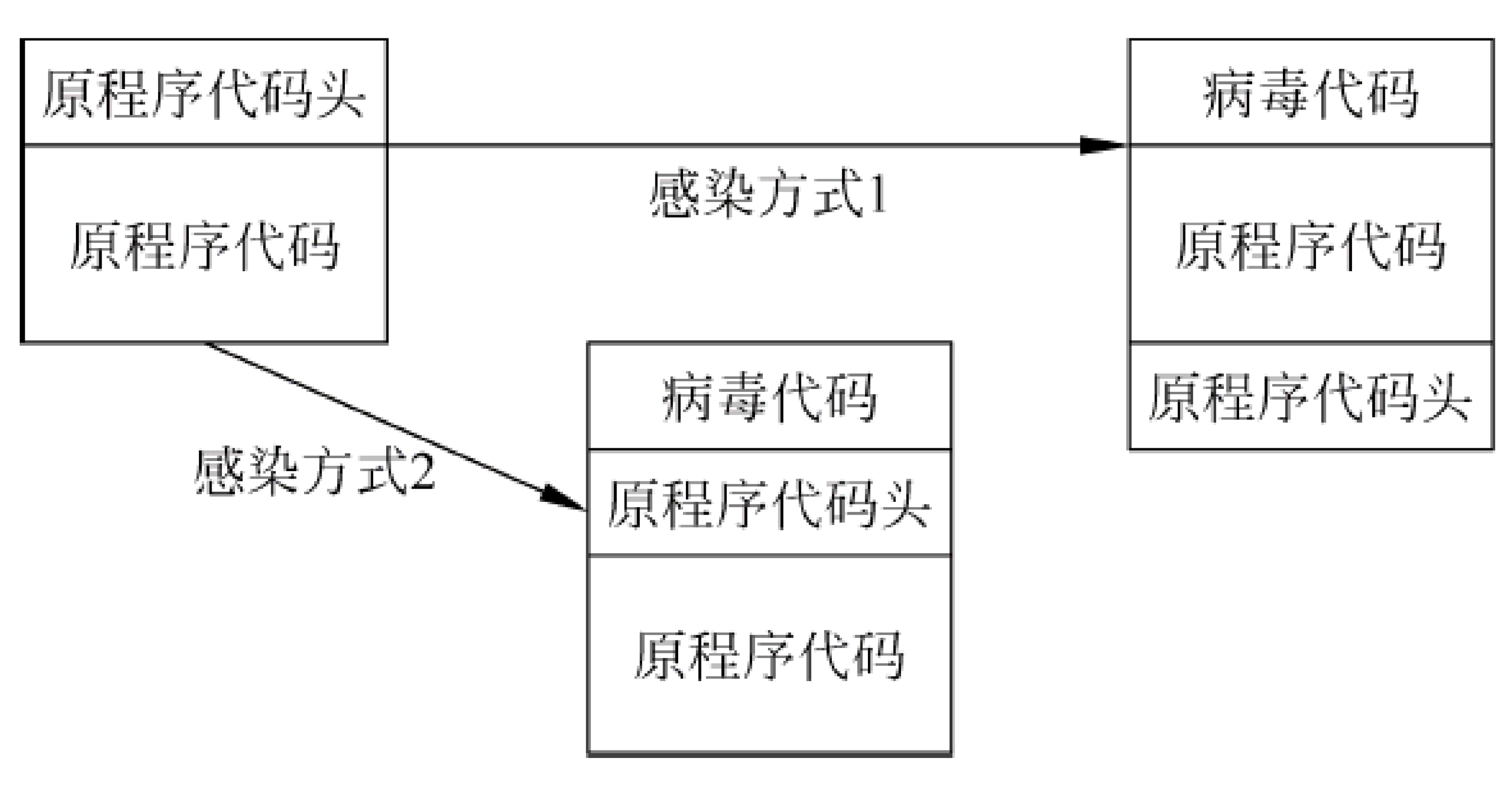


图 4-1 头寄生的方式

随着病毒编码水平的提高,很多感染 DOS 下的 EXE 文件和视窗系统的 EXE 文件的病毒也用了头寄生的方式。为使得被感染的文件仍然能够正常运行,病毒在执行原来程序之前会还原出原来没有感染过的文件用来正常执行,执行完毕之后再进行一次感染,保证硬盘上的文件处于感染状态,而执行的文件是一切正常的,如图 4-2 所示。

2. 尾寄生

由于在头部寄生不可避免地会遇到重新定位的问题,所以最简单也是最常用的寄生方法是直接将病毒代码附加到可执行程序的尾部。对于 DOS 环境下 COM 可执行文件来说,

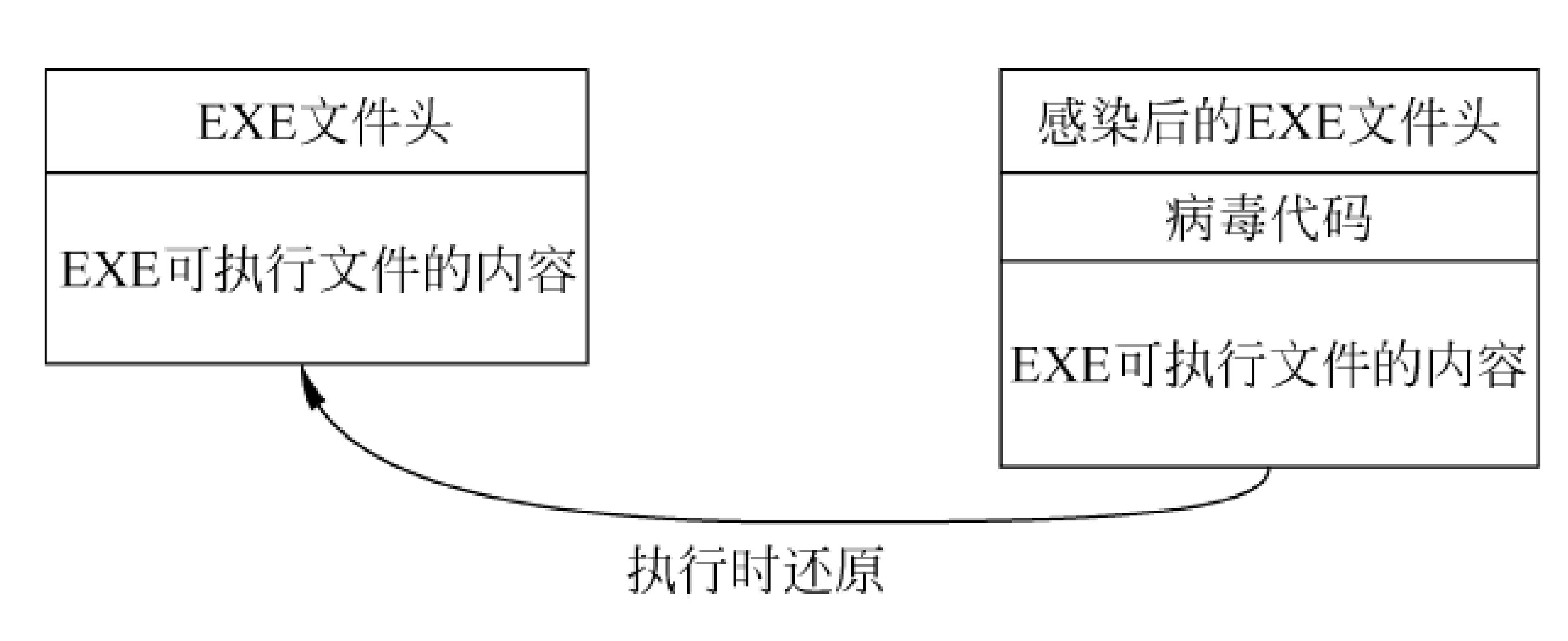


图 4-2　EXE 文件头寄生方式

由于 COM 文件就是简单的二进制代码，没有任何结构信息，所以可以直接将病毒代码附加到程序的尾部，然后改动 COM 文件开始的三个字节为跳转指令，如图 4-3 所示。

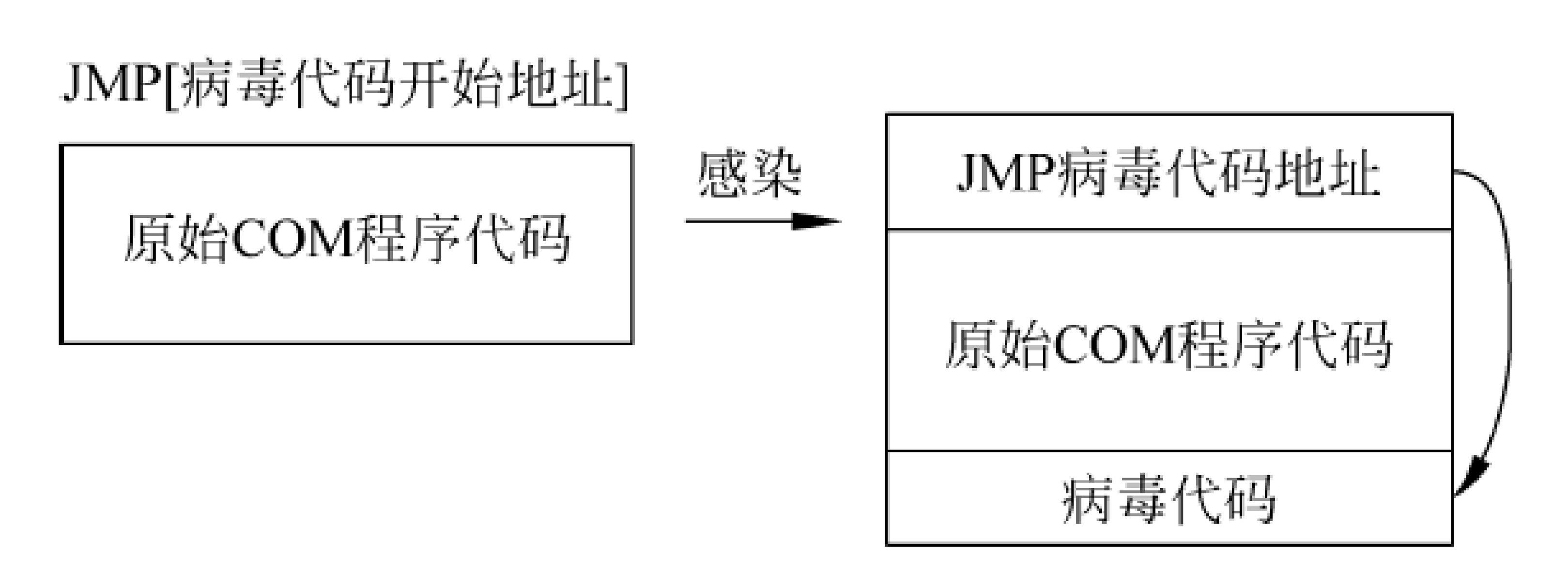


图 4-3　COM 文件的尾寄生

对于 DOS 环境下的 EXE 文件，有两种处理的方法，一种是将 EXE 格式转换成 COM 格式再进行感染；另外一种是修改 EXE 文件的文件头，一般会修改下面几个部分：

（1）代码的开始地址；

（2）可执行文件的长度；

（3）文件的 CRC 校验值；

（4）堆栈寄存器的指针。

对于 Windows 操作系统下的 EXE 文件，病毒感染后同样需要修改文件头。这次修改的是 PE 或者 NE 的头。相对于 DOS 下 EXE 文件的头来说，这项工作要复杂很多，需要修改程序入口地址、段的开始地址、段的属性等，如图 4-4 所示。由于这项工作的复杂性，很多病毒在编写感染代码时会包含一些小错误，造成这些病毒在感染文件时出错，无法继续，从而造成这些病毒无法大规模地传播。

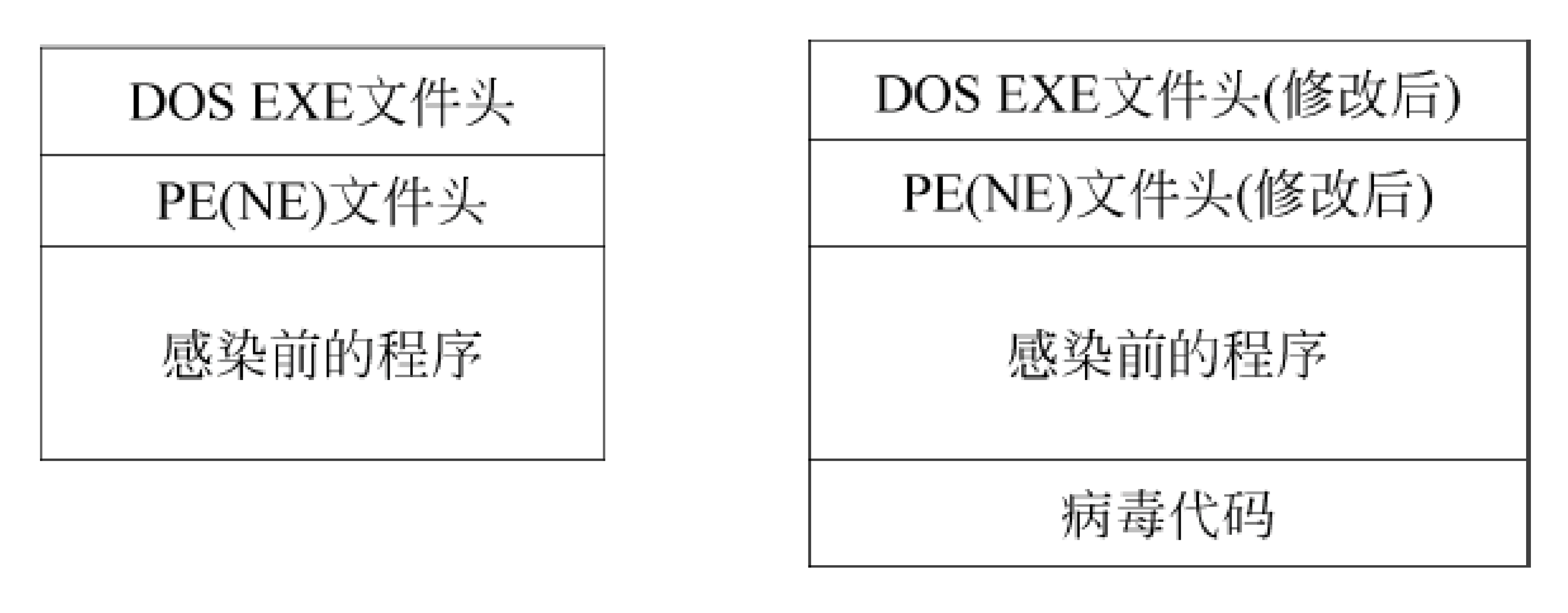


图 4-4　感染前后代码对比

感染 DOS 环境下设备驱动程序（SYS 文件）的病毒会在 DOS 启动之后立刻进入系统，而且对于随后加载的任何软件（包括杀毒软件）来说，所有的文件操作（包括可能的查病毒和杀病毒操作）都在病毒的监控之下。在这种情况下，干净地清除病毒基本上是不可能的。

3. 插入寄生

病毒将自己插入被感染的程序中，可以整段地插入，也可以分成很多段，有的病毒通过压缩原来的代码的方法，保持被感染文件的大小不变。对于中间插入来说，前面论述的更改文件头等基本操作同样需要，而且要求程序的编写更加严谨。所以采用这种方式的病毒相对比较少，即使采用了这种方式，很多病毒也由于程序编写上的错误没有真正流行起来。插入寄生方式如图 4-5 所示。

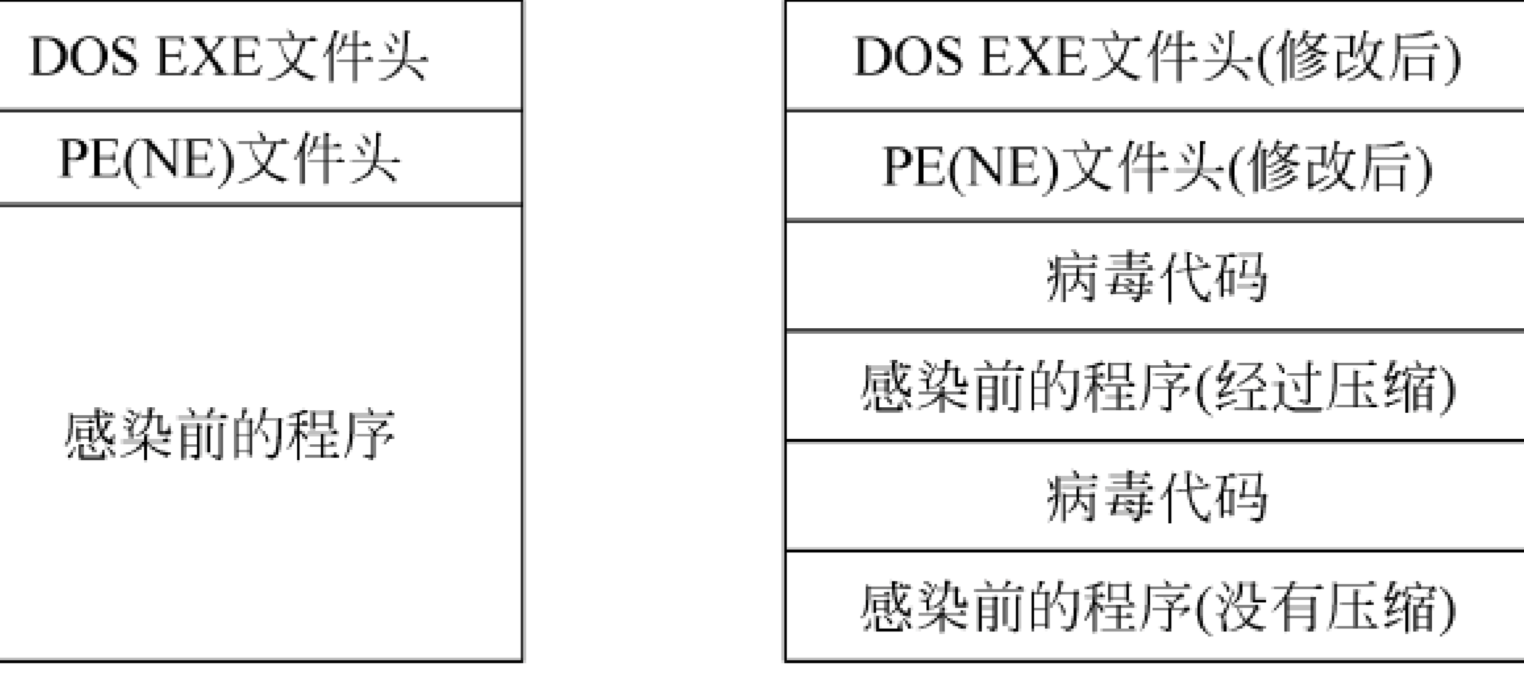


图 4-5　插入寄生方式

4. 空洞利用

对于 Windows 环境下的可执行文件，空洞利用是很有创意的方式。CIH 病毒使用了此方式，CIH 病毒的空洞利用如图 4-6 所示。

感染CIH病毒之前	感染CIH病毒之后
DOS的MZ的文件头	DOS的MZ的文件头
DOS的实模式存根程序(在DOS下执行Windows程序时使用这个存根程序)	DOS的实模式存根程序(在DOS下执行Windows程序时使用这个存根程序)
PE文件标志(00PE0000)	PE文件标志(00PE0000)
PE文件头	PE文件头
PE文件可选头	PE文件可选头(被修改)
.text正文段的头	.text正文段的头(被修改)
.bss堆栈段的头	.bss堆栈段的头(被修改)
.data数据段的头	.data数据段的头(被修改)
.rdata资源数据段的头	.rdata资源数据段的头
...其他段的头	...其他段的头
文件头上的自由空间	病毒块链表指针区 CIH病毒首块
正文段	正文段
自由空间	CIH病毒块2
堆栈段	堆栈段
自由空间	CIH病毒块3
数据段	数据段
自由空间	CIH病毒块4

图 4-6　CIH 病毒的空洞利用

CIH 病毒的首块程序是插在 PE 文件头的自由空间内的。通常 PE 格式文件头的大小为 1024 字节，而 MZ(DOS 可执行文件头)为 128 字节，PE 文件头(包括 PE 文件的标志)为 24 字节，PE 可选文件头为 224 字节，以上共 376 字节。“程序段头”区域大小是根据程序段的数量来确定的，但每个程序段头的大小是固定的，为 40 字节。一般情况下，一个 PE 可执行文件有 5～6 个段，这样计算下来，整个文件头有 408～448 字节的自由空间提供给病毒使用，剩余的病毒代码分块依次插入到各段的自由空间里。

寄生病毒精准地体现了病毒的定义，“寄生在宿主程序上，并且不破坏宿主程序的正常功能”。寄生病毒设计的初衷是希望能够完整地保存原来程序的所有内容，因此除了某些由于程序设计失误造成原来的程序不能恢复的病毒以外，寄生型病毒基本上都是可以安全清除的。

4.3.2 驻留技术

大部分病毒都包括了内存驻留的部分，当被感染的文件被执行之后，病毒的一部分功能模块进入内存，并且一直驻留在那里，即使程序执行完毕。

1. DOS 环境下的内存驻留

标准 DOS 下的终止及驻留程序有两种方法，一种是通过 CONFIG. SYS 作为设备驱动加载；另外一种是调用 DOS 中断 INT21H 的退出但仍然驻留功能。但是病毒不是常规的驻留程序，它通常会使用更加巧妙的方法驻留内存，图 4-7 所示为一些病毒经常隐身的地方。

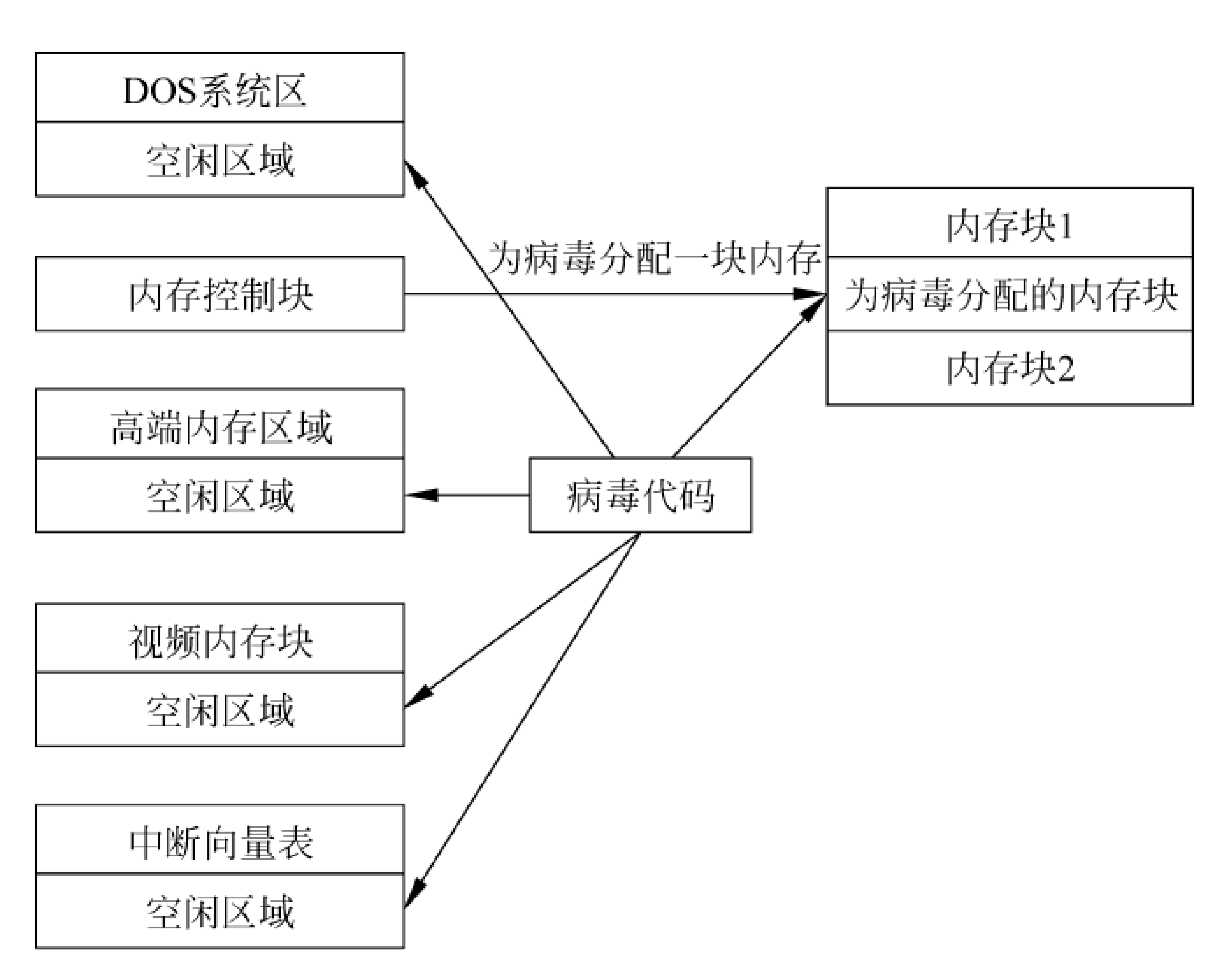


图 4-7　DOS 系统示意图

DOS 环境下的内存驻留病毒会修改大量的 DOS INT21H 功能，根据调用所处理的文件后缀名或者文件类型决定是否进行感染。内存驻留病毒在装入内存中之后，需要使用一种方式告诉随后执行的被感染文件，内存中已经加载了病毒代码，不需要再把病毒放到内存中了。可由下面两种简单的方式达到这个目的。

(1) 修改某些中断,增加一个功能号,如中断 21H,增加一个 AX=FFFFH 的调用,如果返回 1,表示病毒存在,如病毒不存在,DOS 会返回 0。

(2) 在一些很少使用的内存区域中,放置病毒存在的标志。

有一些内存驻留病毒,如使用病毒制造库生成的病毒,由于不正确地使用了防止病毒重新加载的算法,使病毒反复加载,这样会造成其中的一个内存驻留病毒不能正常工作。如果加载的次数过多,会使系统内存耗尽,造成死机。

2. 引导区的内存驻留

引导区内存驻留程序使用类似的方法将病毒代码放入系统内存中,这样会造成系统可用内存减少。由于引导病毒通常都比较小,所以一般减少的内存只有 1KB 或者几 KB。

为了避免用户轻易地觉察到系统可用内存的减少,一些病毒会等待 DOS 完全启动成功,然后使用 DOS 自己的功能分配内存。这样不会显示整个可用内存减少,而是在 DOS 可用的内存中增加了一个小的常驻程序,往往不会引起用户的警觉。

3. Windows 环境下的内存驻留

Windows 环境下的病毒驻留技术是在内存中寻找合适的页面并将病毒自身拷贝到其中,而且在系统运行期间能够始终保持病毒代码的存在。例如,CIH 病毒调用 INT20 中断,使用 VxD call Page Allocate 系统调用,请求系统分配两个 PAGE 大小的 Windows 系统内存,用于驻留病毒代码。

4.3.3 加密变形技术

随着病毒技术的发展,出现了一类新的病毒——加密病毒。这类病毒的特点是:其入口处具有解密子,而病毒主体代码被加密。病毒运行时,首先由得到控制权的解密代码对病毒主机进行循环解密,完成后将控制权交给病毒主机运行。病毒主体感染文件时,会将解密子用随机密钥加密过的病毒主体,以及保存在病毒体内或嵌入解密子中的密钥一同写入被感染文件。但是加密病毒不同传染实例的解密子仍然保持不变的机器码明文,所以应用特征码查毒技术,仍是一种有效的检测方法。由于加密病毒还没有能够完全逃脱特征码扫描,所以天才的病毒作者们在加密病毒的基础之上进行改进,使解密子的代码对不同传染实例呈现出多样性,这就出现了加密变形病毒。它和加密病毒非常相似,唯一的改进在于病毒主体在感染不同文件时会构造出一个功能相同但代码不同的解密子,也就是不同传染实例的解密子具有相同的解密功能,但代码却截然不同。比如,一条指令完全可以拆成几条来完成,中间可能会被插入无用的垃圾代码,以及使用随机的寄存器、加密长度等。由于无法找到不变的特征码,特征码扫描技术就彻底失效了。

图 4-8 所示为一段最简单的加密变形病毒代码,这段代码的作用是将预先加密的病毒代码解密,然后跳转到执行感染和破坏功能的病毒代码中。

这段解密的代码和加密后的病毒都是在感染的时候动态生成的。我们可以看到,使用的寄存器、密钥、加密代码的长度等,甚至解密使用的指令都是随机的。所以指望能够从这些代码中找到固定的病毒特征码是徒劳的,也就是由于这种加密变形病毒的出现,使利用简单特征码进行病毒检测的技术走到了尽头。

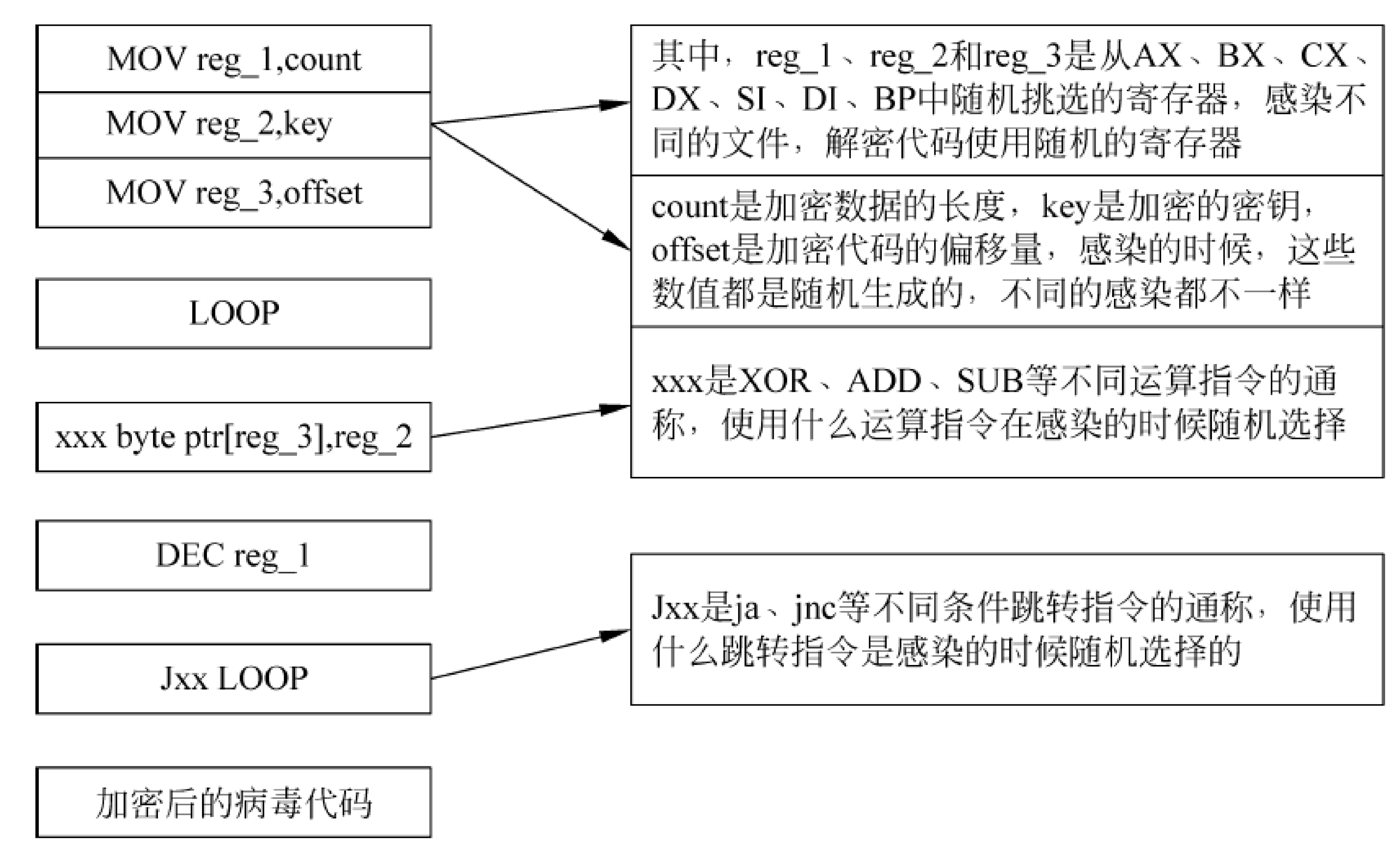


图 4-8　加密变形病毒代码

4.3.4　隐藏技术

病毒在进入用户系统之后，会采取种种方法隐藏自己的行踪，让用户无法感觉到它的存在。引导型病毒、文件型病毒以及 Windows 环境下的病毒采用了不同的技术达到这个目的。

1. 引导型病毒的隐藏技术

引导型病毒的隐藏有以下两种基本的方法。

(1) 改变基本输入输出系统(BIOS)中断 13H 的入口地址，使其指向病毒代码之后，发现调用 INT13H 被感染扇区请求的时候，将原来没有被感染过的内容返回给调用的程序。因此，任何 DOS 程序都无法觉察到病毒的存在，如果反病毒软件无法首先将内存中的病毒清除的话，同样无法清除这种病毒。此种隐藏技术详见图 4-9 所示。

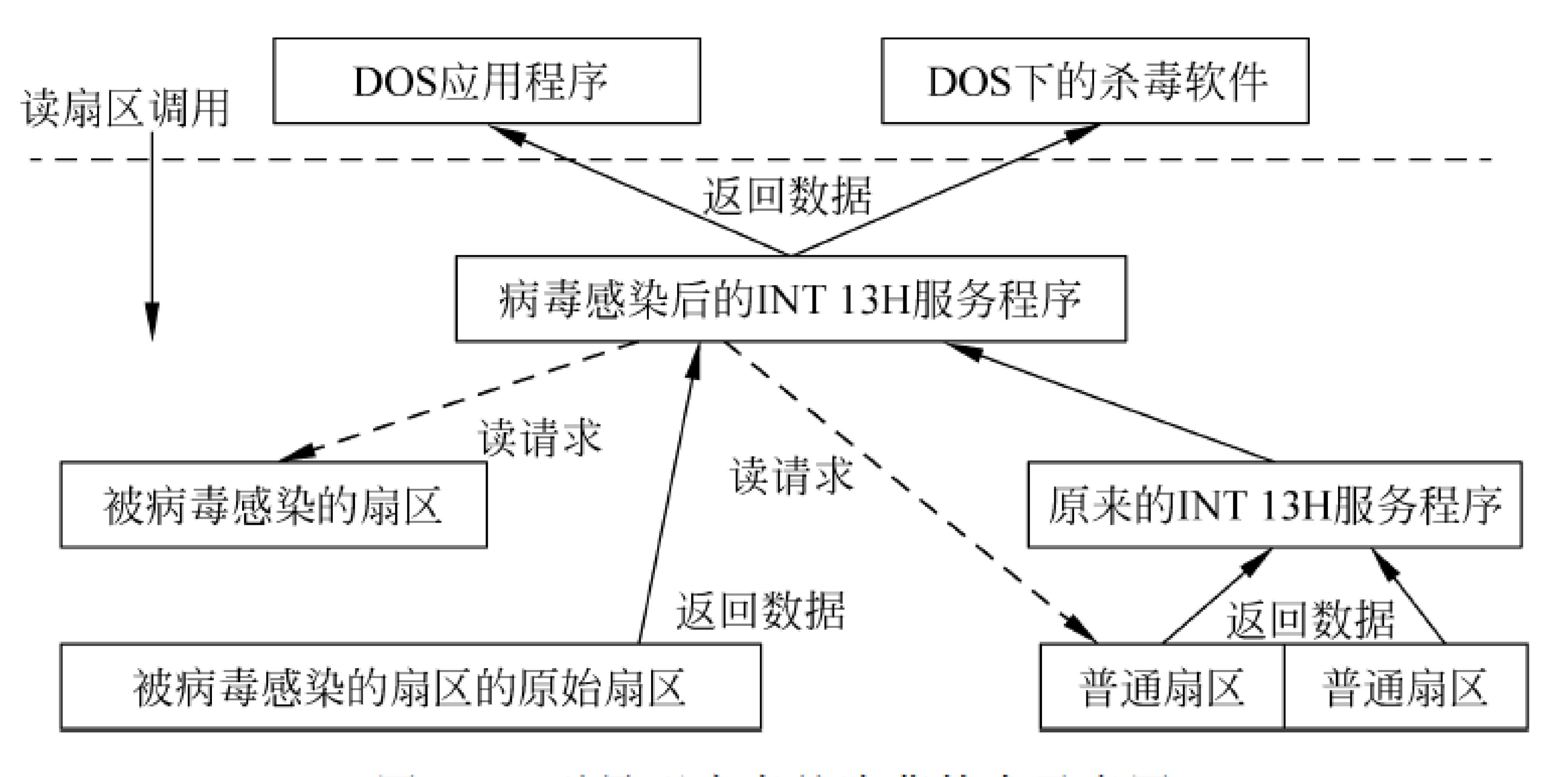


图 4-9　引导型病毒的隐藏技术示意图

(2) 另外一种更高明的方法是直接针对杀毒软件的。为了对付上面所说的病毒隐藏手段，一些杀毒软件采用直接对磁盘控制器进行操作的方法读写磁盘扇区。病毒的制造者在加载程序的时候制造假象，当启动任何程序的时候，修改 DOS 执行程序的中断功能。首先

把被病毒感染的扇区恢复原样，这样即使反病毒程序采用直接磁盘访问也只能看到正常的磁盘扇区，当程序执行完成后，再重新感染，详见图 4-10 所示。对付这种病毒的唯一方法是在进行病毒检测之前首先清除内存中的所有病毒。

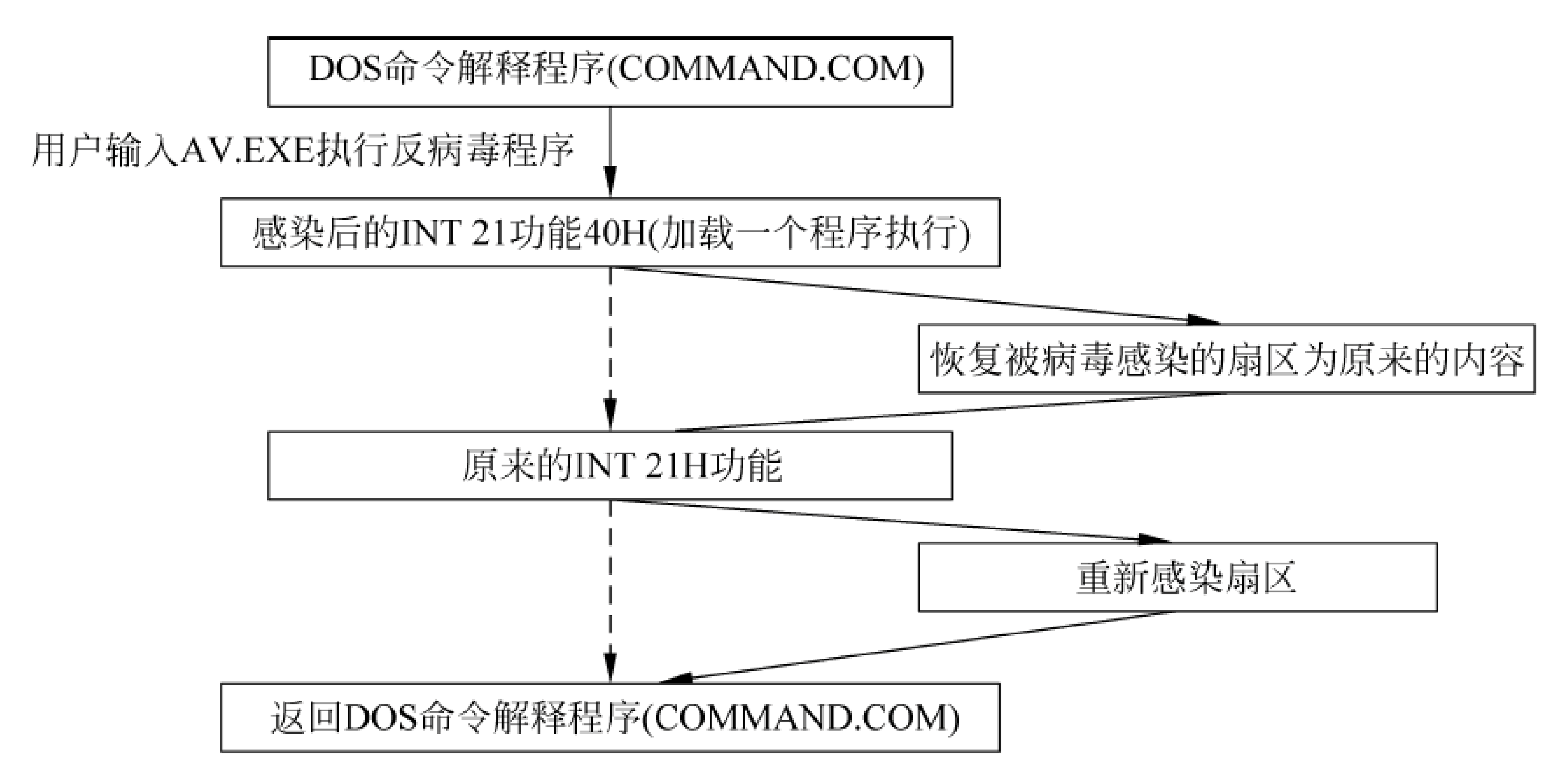


图 4-10　引导型病毒感染过程

引导型病毒为了隐藏自己，经常采用更改活动引导记录，使病毒代码看起来类似于正常启动代码等方法，尽可能减少被杀毒软件发现的可能性。

2. 文件型病毒的隐藏技术

文件型病毒的隐藏技术和引导型病毒的隐藏技术相似，同样是替换 DOS 或者基本输入输出系统的文件系统相关调用。在打开文件时将文件的内容恢复至未感染的状态，在关闭文件时重新进行感染。

由于访问文件型病毒的方式非常多，所以实现完全的文件型病毒隐藏是一件非常困难的任务，一个完整的隐藏技术应该包括以下几个方面的处理，如图 4-11 所示。

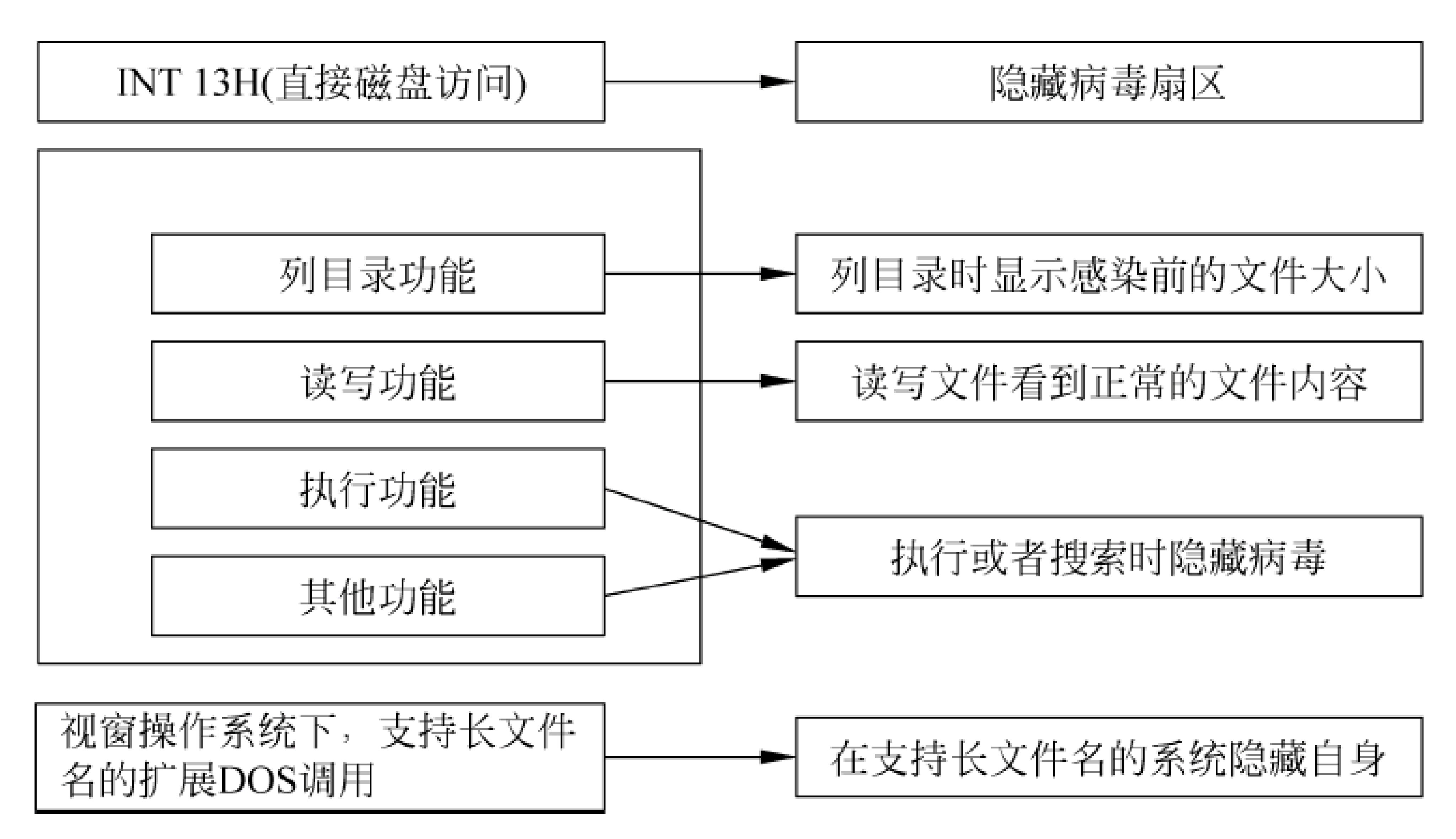


图 4-11　文件型病毒的隐藏技术

一般的文件型病毒仅仅使用其中的一部分隐藏技术。最常见的是对列目录进行隐藏，因此，在使用 DIR 命令列目录的时候，看到的文件大小是病毒提供的，从实际大小减去病毒大小的数值，这样就不会感觉到病毒的存在。

3. Windows 环境下的病毒隐藏技术

在 Windows 系统中，有一定经验的用户觉察系统异常后，常常使用管理器进程列表来观察是否有异常进程的存在。若存在，则会采取一定的防范措施。因此，实现进程或模块隐藏应该是一个成功病毒所必须具备的特征。在 Windows 9x 下，Kernel32. dll 有一个可以使进程从管理器进程列表中消失的导出函数 RegisterServiceProcess，但它仍不能使病毒逃离一些进程浏览工具的监视。当病毒编写者知道这些工具是如何来枚举进程后，就能找到对付这些工具的相应方法。

4.4 计算机病毒的检测与防范

由于计算机病毒具有相当的复杂性和行为不确定性，计算机病毒的检测与防范需要多种技术综合应用。

4.4.1 计算机病毒的检测

对系统进行检测，可以及时掌握系统是否感染病毒，以及被感染的情况，以便于及时对症处理。检测病毒的方法有：特征代码法、校验和法、行为监测法、软件模拟法。

1. 特征代码法

特征代码法是检测已知病毒最简单、最经济的方法。特征代码法的实现步骤如下。

(1) 采集已知病毒样本，病毒如果既感染 COM 文件，又感染 EXE 文件，对这种病毒要同时采集 COM 型病毒样本和 EXE 型病毒样本。

(2) 在病毒样本中，抽取特征代码。

(3) 打开被检测文件，在文件中搜索，检查文件中是否含有病毒数据库中的病毒特征代码，如果发现病毒特征代码，由于特征代码与病毒一一对应，便可以断定出被查文件中感染的是何种病毒。

特征代码法的特点是：速度慢，随着病毒种类的增多，检测时间变长；误报率低；不能检查多态型病毒；不能检测隐藏型病毒。

2. 校验和法

校验和法指在使用文件前或定期地检查文件内容前后的校验和变化，以此来判断文件是否被感染的一种方法。

运用校验和法检测病毒采用以下三种方式。

(1) 在检测病毒工具中纳入校验和法，对被检测的对象文件计算其正常状态的校验和，将校验和值写入被查文件的检测工具中，而后进行比较。

(2) 在应用程序中，放入校验和法自我检查功能，将文件正常状态的校验和写入文件自身中，每当应用程序启动时，比较现行校验和与原校验和值，实现应用程序的自检测。

(3) 将校验和检测程序常驻内存，每当应用程序开始运行时，自动比较检测应用程序内部或别的文件中预先保存的校验和。

校验和法的特点是：方法简单，能发现未知病毒、被检测文件的细微变化；可以报警；不能识别病毒名称；不能检测隐藏型病毒。

3. 行为监测法

行为监测法是利用病毒的特有行为特征来监测病毒的方法。通过对病毒多年的观察和研究，有一些行为是病毒的共同行为，而且比较特殊。在正常程序中，这些行为比较罕见，当程序运行时，监视其行为，如果发现了病毒行为，立即报警。

行为监测法的特点是：可发现未知病毒；可相当准确地预报未知的多数病毒；可能误报警；不能识别病毒名称；实现时有一定难度。

4. 软件模拟法

软件模拟法是一种软件分析器，用软件方法来模拟和分析程序的运行。新型检测工具纳入了软件模拟法，该类工具开始运行时，使用特征代码法检测病毒，如果发现疑似隐藏型病毒或多态型病毒时，启动软件模拟模块，监视病毒的运行，待病毒自身的密码译码以后，再运用特征代码法来识别病毒的种类。

4.4.2 计算机病毒的防范

由于在计算机病毒的处理过程中，存在对症下药的问题，即只能是发现一种病毒以后，才可以找到相应的治疗方法，因此处理病毒具有很大的被动性。而防范计算机病毒，则可掌握工作的主动权，所以应把工作重点放在计算机病毒的预防上。防范计算机病毒主要从管理和技术两方面着手。

1. 严格的管理

制定相应的管理制度，避免蓄意制造、传播病毒的事件发生。例如，对接触重要计算机系统的人员进行选择和审查；对系统的工作人员和资源进行访问权限划分；对外来人员上机或外来磁盘的使用严格限制，特别是不准用外来系统盘启动系统；规定下载的文件要经过严格检查，甚至规定下载文件、接收 E-mail 等需要使用专门的终端和账号；接收到的程序要严格限制执行等。

2. 有效的技术

除管理方面的措施外，采取有效的技术措施防止计算机病毒的感染和蔓延也是十分重要的。计算机病毒预防是指在病毒尚未入侵或刚刚入侵时，就拦截、阻止病毒的入侵或立即报警。目前在预防病毒工具中采用的技术主要有如下 6 种。

(1) 将大量的杀毒软件汇集一体，检查是否存在已知病毒。

(2) 检测一些病毒经常要改变的系统信息，如引导区、中断向量表、可用内存空间等，以确定是否存在病毒的行为。

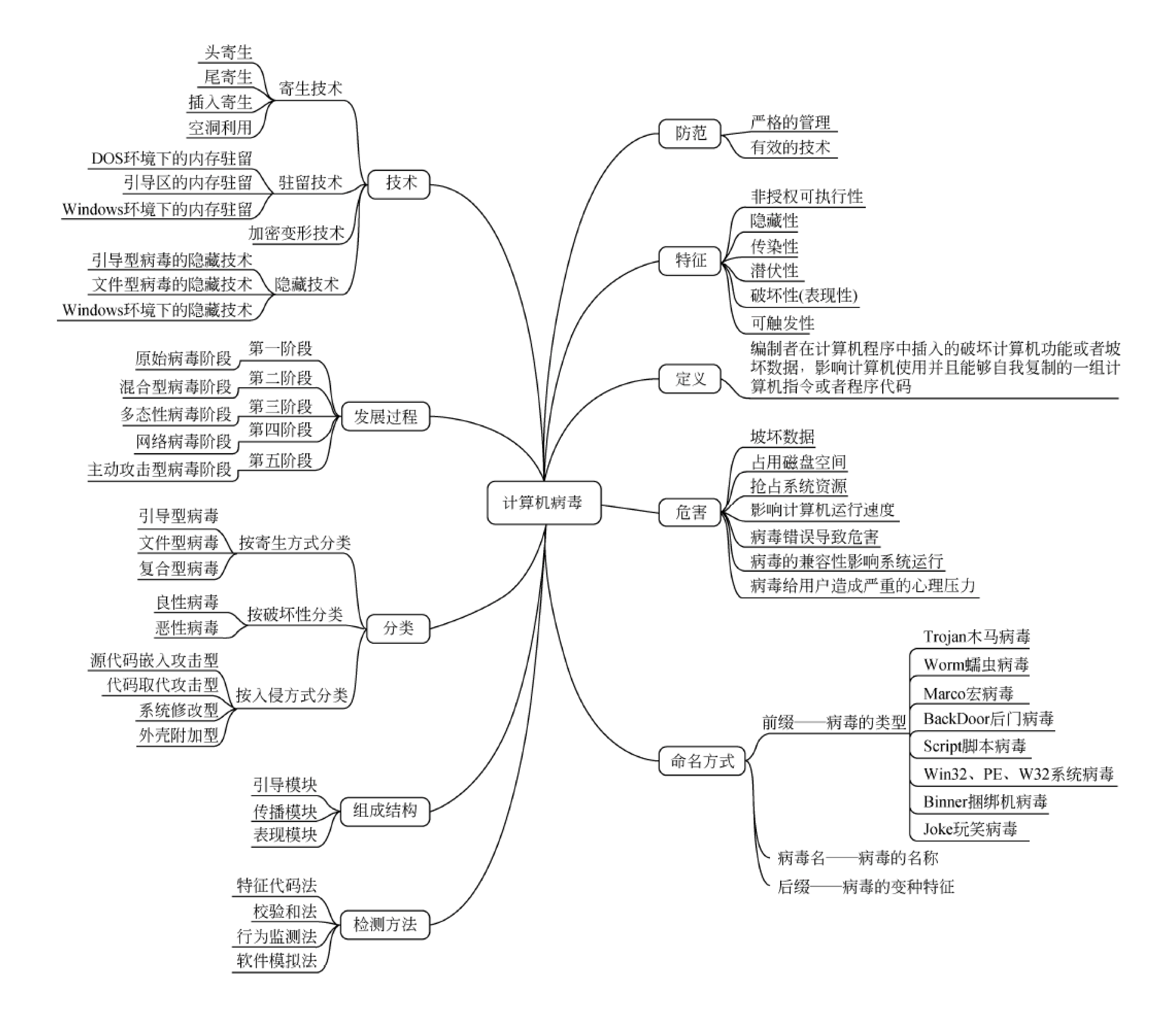
(3) 监测写盘操作，对引导区或主引导区的写操作报警。

(4) 对计算机系统中的文件形成一个密码校验码和实现对程序完整性的验证，在程序执行前或定期对程序进行密码校验，如有不匹配现象立即报警。

(5) 智能判断，设计病毒行为过程判定知识库，应用人工智能技术，有效区分正常程序与病毒程序的行为，是否误报警取决于知识库选取的合理性。

(6) 智能监测，设计病毒特征库，病毒行为知识库，受保护程序存取行为知识库等多个知识库及相应的可变推理机。通过调整推理机，能够对付新类型病毒，这也是未来预防病毒技术发展的方向。

4.5 本章小结



4.6 习　　题

一、填空题

1. 计算机病毒结构一般由(　　)、传播模块和表现模块三部分构成。

2. (　　)技术是文件型病毒最常用的传染方法。

3. 病毒寄生技术可以分为头寄生、尾寄生、插入寄生和(　　)4 种。

4. (　　)是检测已知病毒的最简单、最经济的方法。

5. 计算机病毒采用前后缀法命名，病毒前缀表示(　　)，病毒名表示病毒名称，病毒后缀表示病毒的变种特征。

二、选择题

1. 在计算机病毒发展过程中，(　　)给计算机病毒带来了第一次流行高峰，同时病毒具有了自我保护的功能。

A. 多态性病毒阶段　　　　B. 网络病毒阶段

C. 混合型病毒阶段　　　　D. 主动攻击型病毒阶段

2. 蠕虫病毒是最常见的病毒，有其特定的传染机理，它的传染机理是(　　)。

A. 利用网络进行复制和传播　　B. 利用网络进行攻击

C. 利用网络进行后门监视　　D. 利用网络进行信息窃取

3. (　　)是一种更具破坏力的恶意代码，能够感染多种计算机系统，其传播之快、影响范围之广、破坏力之强都是空前的。

A. 特洛伊木马　　B. CIH 病毒

C. CoDeReDⅡ双型病毒　　D. 蠕虫病毒

4. 按照计算机病毒的链接方式不同分类，(　　)是将其自身包围在合法的主程序的四周，对原来的程序不做修改。

A. 源码型病毒　　B. 外壳型病毒

C. 嵌入式病毒　　D. 操作系统型病毒

5. 下面属于蠕虫病毒的是(　　)。

A. Worm. Sasser 病毒　　B. Trojan. QQPSW 病毒

C. Backdoor. IRCBot 病毒　　D. Macro. Melissa 病毒

6. 杀毒软件报告发现病毒 Macro. Melissa，由该病毒名称可以推断出病毒类型是(　　)，这类病毒的主要感染目标是(　　)。

A. 文件型　　B. 引导型　　C. 目标型　　D. 宏病毒

E. EXE 或 COM 可执行文件　　F. Word 或 Excel 文件

G. DLL 系统文件　　H. 磁盘引导区

7. 计算机病毒通常是指(　　)。

A. 一段程序　　B. 一条命令　　C. 一个文件　　D. 一个标记

8. 文件型病毒传染的对象主要是以下(　　)文件类型。

A. DBF　　B. WPS

C. COM 和 EXE　　D. EXE 和 DOC

9. 计算机病毒具有(　　)。

A. 传播性、潜伏性、破坏性　　B. 传播性、破坏性、易读性

C. 潜伏性、破坏性、易读性　　D. 传播性、潜伏性、安全性

10. 目前使用的防杀病毒软件的作用是(　　)。

A. 检查计算机是否感染病毒，并消除已感染的任何病毒

B. 杜绝病毒对计算机的侵害

C. 检查计算机是否感染病毒，并清除部分已感染的病毒

D. 查出已感染的任何病毒，清除部分已感染的病毒

11. 在计算机病毒检测手段中，下面关于特征代码法的表述，错误的是(　　)。

A. 随着病毒种类增多，检测时间变长　　B. 可以识别病毒名称

C. 误报率低　　D. 可以检测出多态型病毒

12. 下面关于计算机病毒的说法中，错误的是(　　)。

A. 计算机病毒只存在于文件中

B. 计算机病毒具有传染性

C. 计算机病毒能自我复制

D. 计算机病毒是一种人为编制的程序

13. 以下方法中，不适用于检测计算机病毒的是（　　）。
A. 特征代码法　B. 校验和法　C. 加密法　D. 软件模拟法

14. 下列不属于行为检测法检测病毒的行为特征的是（　　）。
A. 占有 INT 13H　B. 修改 DOS 系统内存总量
C. 病毒程序与宿主程序的切换　D. 不使用 INT 13H

15. 下列计算机病毒检测手段中，主要用于检测已知病毒的是（　　）。
A. 特征代码法　B. 校验和法　C. 行为检测法　D. 软件模拟法

16. 计算机病毒检测手段中，校验和法的优点是（　　）。
A. 不会误报　B. 能识别病毒名称
C. 能检测出隐蔽性病毒　D. 能发现未知病毒

17. 关于特征代码法，下列说法错误的是（　　）。
A. 采用特征代码法检测准确
B. 采用特征代码法可识别病毒的名称
C. 采用特征代码法误报率高
D. 采用特征代码法能根据检测结果进行解毒处理

18. 对于采用校验和法检测病毒的技术，下列说法正确的是（　　）。
A. 可以识别病毒类型　B. 可以识别病毒名称
C. 常常误警　D. 误警率低

19. 以下描述的现象中，不属于计算机病毒的是（　　）。
A. 破坏计算机的程序或数据
B. 使网络阻塞
C. 各种网上欺骗行为
D. Windows“控制面板”中无“本地”连接图标

三、判断题

1. 按照病毒的传播媒介分类，计算机病毒可分为单机病毒和网络病毒。
2. 防范计算机病毒主要从管理和技术两方面着手。
3. 计算机病毒只会破坏计算机的操作系统，而对其他网络设备不起作用。
4. 计算机病毒不影响计算机的运行速度和运算结果。
5. 蠕虫既可以在互联网上传播，也可以在局域网上传播，而且由于局域网本身的特性，蠕虫在局域网上传播速度更快，危害更大。

四、简答题

1. 什么是计算机病毒？
2. 计算机病毒的组织结构有哪些？
3. 计算机病毒的特征有哪些？
4. 按计算机病毒的命名规则，解释说明病毒 troj. generic. apc 的各字段的含义。
5. 给出计算机病毒的 4 种检测方法。

第5章　身份认证与访问控制技术

【本章学习目标】

- 理解身份认证的概念
- 了解常用身份认证方式
- 理解访问控制的概念
- 掌握自主访问控制、强制访问控制及基于角色的访问控制模式
- 了解数字签名的概念
- 掌握数字签名原理
- 掌握原文加密的数字签名实现方法

在当前开放式的网络环境中,任何在网络上的通信都可能遭到黑客的攻击,窃听机密消息,伪造、复制、删除和修改消息等攻击越来越多。所有的攻击都可能对正常通信造成破坏性的影响,给在线电子交易和网银的安全性带来极大的挑战。各种层出不穷的计算机犯罪案件引发了人们对网络身份的信任危机,证明访问用户身份及防止身份被冒名顶替变得极为重要。身份认证技术和访问控制技术是网络安全的最基本要素,是用户登录网络时保证其使用和交易“门户”安全的首要条件。

5.1　身份认证技术

5.1.1　身份认证概述

1. 身份认证概念

认证(Authentication)是指通过对网络系统使用过程中的主客体双方互相鉴别确认身份后,对其赋予恰当的标志、标签和证书等的过程。认证可以解决主体本身的信用问题和客体对主体访问的信任问题。认证可以为下一步的授权奠定基础,是对用户身份和认证信息的生存、存储、同步、验证和维护的全生命周期的管理。

身份认证(Identity and Authentication Management)是网络用户在进入系统或访问不同保护级别的系统资源时,系统确认该用户的身份是否真实、合法和唯一的过程。

2. 身份认证作用

在网络系统中,身体认证是网络安全中的第一道防线,极为重要,是其他安全机制的基石。如图5-1所示,用户在访问系统前,先要经过身份认证系统进行身份识别,可以通过访问监控设备(系统),根据用户的身份和授权数据库,确定所访问系统资源的权限。授权数据

库由安全管理员按照需要配置。审计系统根据设置记载用户的请求和行为。访问控制和审计系统都依赖于身份认证系统提供的“认证信息”鉴别和审计。

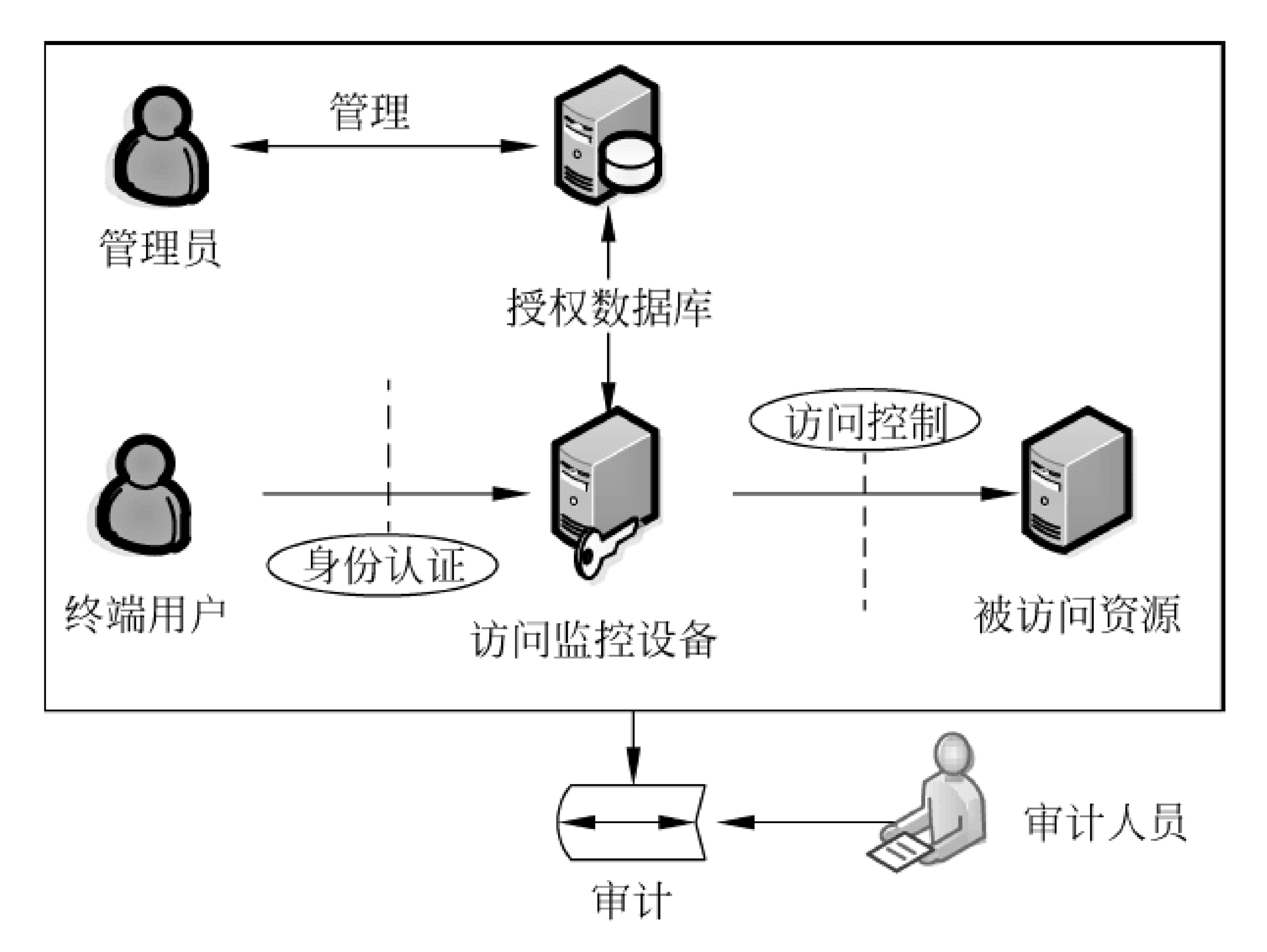


图 5-1　身份认证和访问控制过程

5.1.2　身份认证方式

网络系统中常用的身份认证方式主要有静态密码认证、动态口令认证、USB Key 认证、生物识别认证和 CA 认证等。

1. 静态密码认证

静态密码方式是指以用户名及密码认证的方式，是最简单、应用最广泛的身份认证方法。所有用户的密码由用户自己设定，只有用户本人知道。只要能够正确输入密码，信息系统就认为操作者是合法用户，其安全性在很大程度上依赖于密码强度。实际上，很多用户为了方便起见，经常使用生日、电话号码等具有用户自身特征的字符串作为密码，为系统安全留下隐患。同时，由于密码是静态数据，在验证过程中需要在网络介质中传输，很容易被木马程序或监听设备截获。因此，用户名及密码方式是安全性比较低的身份认证方式。

2. 动态口令认证

动态口令是应用较广的一种身份认证方法，采用哈希算法产生。基于动态口令的认证方式主要有动态短信密码和动态口令牌两种方式。口令一次一密，每次登录都用不同的密码，可以避免口令丢失的逻辑漏洞。前者是将系统发给用户注册手机的动态短信密码进行身份认证，后者则以发给用户动态口令牌进行认证，如图 5-2 所示。动态口令认证方式不需要用户定期修改密码，无须担心密码泄露，该认证方式广泛应用在 VPN、网上银行及电子商务等领域。

3. USB Key 认证

USB Key(U 盾)认证方式近几年得到了广泛应用。它主要采用软硬件相结合、一次一密的强双因素认证模式，很好地解决了安全性与易用性之间的矛盾。该方式以一种 USB 接口的硬件设备，内置单片机或智能卡芯片，可存储用户的密钥或数字证书，利用其内置的密码算法实现对用户身份的认证。其身份认证系统主要有两种认证模式：基于冲击/响应模式和基于 PKI 体系的认证模式。常用的网银 USB Key 如图 5-3 所示。



图 5-2　动态口令牌


图 5-3　网银 USB Key

4. 生物识别认证

生物识别认证是指通过可测量的生物信息和行为等特征进行身份认证的一种技术。认证系统测量的生物特征一般是用户唯一生理特征或行为方式。生物特征分为身体特征和行为特征两类。身体特征包括指纹、掌形、视网膜和 DNA 等；行为特征包括签名、语音和行走步态等。

5. CA 认证

CA(Certification Authority)是国际认证机构的通称，是对申请用户进行发放、管理、校验或取消数字证书的机构。CA 认证用于审查证书持有者身份的合法性，并签发管理证书，以防止证书被伪造或篡改。如表 5-1 所示，其发放、管理和认证是一个复杂的过程，即 CA 认证过程。

表 5-1　证书的类型与作用

证书名称	证书类型	主要功能描述
个人证书	个人证书	个人网上交易、网上支付、电子邮件等
单位证书	单位身份证书	用于企事业单位网上交易、网上支付等
	E-mail 证书	用于企事业单位内安全电子邮件通信
	部门证书	用于企事业单位内某个部门的身份认证
服务器证书	企业证书	用于服务器、安全站点认证等
代码签名证书	个人证书	用于个人软件开发者对其软件的签名
	企业证书	用于软件开发企业对其软件的签名

CA 作为网络安全可信认证及证书管理机构，其主要职能是管理和维护所签发的证书，并提供各种证书服务，包括证书的签发、更新、回收和归档等。CA 系统的主要功能是管理其辖域内的用户证书，因此，CA 系统功能及 CA 证书的应用将围绕证书进行具体的管理。

5.1.3　身份认证系统

身份认证系统的组成一般包括三个部分：认证服务器、认证系统客户端和认证设备。认证系统主要通过身份认证协议和认证系统软硬件来实现。其中，身份认证协议又分为单向认证协议和双向认证协议。若通信双方只需一方鉴别另一方的身份，则称为单项认证协议；如果双方都需要验证身份，则称为双向认证协议。

AAA(Authentication，Authorization，Accounting)认证系统现阶段应用最为广泛。其中，认证(Authentication)是验证用户身份与可使用网络服务的过程，授权(Authorization)是依据认证结果开放网络服务给用户的过程，审计(Accounting)是记录用户对各种网络操作及服务的用量并进行计费的过程。

5.1.4 身份认证方法

在网络系统中,各用户以数字认证方式确定身份。网络中的各种资源通过认证机制来实现安全保护。认证机制与授权机制经常结合在一起,通过认证的用户才可获得使用权限。互联网最常用的认证方法有固定口令、一次性口令、双因素安全令牌和单点登录等。

1. 固定口令

固定口令认证是网络中最常用的认证系统,是一种以检验用户设定的固定字符串来进行系统认证的方式。当通过网络访问系统资源时,系统要求输入用户名和密码。在账户和密码被确认后,用户便可访问授权的资源。这种认证方式简单,但由于其相对固定,很容易受到多种攻击。而且很多认证系统的口令是未经加密的明文,攻击者通过窃听网络数据,很容易分辨出某种特定系统的认证数据,并提取出用户名和密码。

2. 一次性口令

为了提高固定口令的安全性,出现了一次性口令(One Time Password,OTP)认证体制,即在登录过程中加入不确定因素,使每次登录过程中传送的信息都不相同,从而提高系统安全性。一次性口令认证系统的组成如下。

(1) 生成不确定因子。常用的生成不确定因子的方式有三种:口令序列方式、挑战/回答方式和时间同步方式。

(2) 生成一次性口令。利用不确定因子生成一次性口令的方式有以下两种。

① 硬件卡。在具有计算功能的硬件卡上输入不确定因子,卡中集成的计算逻辑对输入数据进行处理,并将结果反馈给用户作为一次性口令。基于硬件卡的一次性口令大多属于挑战/回答方式,一般配备有数字按键,便于不确定因子的输入。

② 软件。与硬件卡基本原理类似,以软件代替其计算逻辑。软件口令生成方式及灵活性较高,某些软件还可限定用户登录的地点。

3. 双因素安全令牌

双因素身份认证系统由身份认证服务器、安全令牌、认证代理、认证应用开发包等几部分组成。身份认证服务器提供数据存储、AAA 服务、管理等功能,是整个系统的核心部分。安全令牌是重要的双因素认证方式,系统提供多种形式的安全令牌,供不同用户选用。

双因素安全令牌用于生成用户当前登录的动态口令,采用加密算法及可靠设计,可防止读取密码信息。该令牌每 60s 得到一个新动态口令显示在液晶屏上,动态口令具有极高的抗攻击性。

4. 单点登录

单点登录(Single Sign On,SSO)也称单次登录,是在多个应用系统中,用户只需要登录一次就可以访问所有相互信任的应用系统,安全凭证可以在不同的应用系统中共享,是目前比较流行的企业业务整合的解决方案之一。其中,对网络服务器认证由专门的认证服务器负责,并且统一对登录用户授权。

单点登录与传统的登录相比较,优势主要体现在以下 5 个方面。

(1) 管理简单。现有的操作系统实现中,SSO 的相关任务可以作为日常维护工作的一部分,使用与其他任务管理相同的工具来执行。

(2) 管理控制便捷。Windows 中所有的网络管理信息,包括 SSO 的特定信息,都存放

在一个用 Active Directory 组织的存储库中。对每个用户的权限与特权，仅有一个授权列表，使管理员在更改或维护用户特权后，可将结果传送到整个网络系统。

(3) 用户使用简便。用户不用多次登录，也无须在访问网络资源时记住很多密码。

(4) 安全性更高。SSO 可用的方法都提供用户身份验证，并为用户与网络资源的会话加密奠定了基础。它不仅取消了多次访问密码，还降低了用户习惯写或多次输入密码而被盗用密码的危险。此外，由于将网络管理信息并入存储库，管理员还可确认所禁用的用户账号，从而使网络系统的安全性更高。

(5) 合并异构网络。通过连接各种网络，相关的网络管理工作也可以进行合并，从而优化了管理，实现整个系统安全策略统一实施。

5.2 访问控制技术

如果说身份证认证技术解决了用户是“谁”的问题，那么用户“能够做什么”则是由访问控制决定的。访问控制技术作为国际标准化组织定义的 5 项标准安全服务之一，是实现信息系统安全的一项重要机制。美国国防部的可信计算机系统评估标准把访问控制作为评价系统安全的主要指标之一，因此，访问控制对提高系统安全的重要性是不言而喻的。

5.2.1 访问控制概述

1. 访问控制概念

访问控制(Access Control)指系统对用户身份及其所属的预先定义的策略组限制其使用数据资源的能力，通常用于系统管理员控制用户对服务器、目录、文件等网络资源的访问。

访问控制的主要目的是限制访问主体对客体的访问，从而保障数据资源在合法范围内得以有效使用和管理。访问控制包括以下三个要素。

(1) 主体 S(Subject)。指一个提出请求或要求的实体，是动作的发起者，但不一定是动作的执行者。主体可以是某个用户，也可以是用户启动的进程、服务和设备。

(2) 客体 O(Object)。是授受其他实体访问的被动实体。客体的概念也很广泛，凡是可以被操作的信息、资源、对象都可以认为是客体。在信息社会中，客体可以是信息、文件、记录等的集合体，也可以是网络的硬件设施，无线通信中的终端，甚至一个客体可以包含另一个客体。

(3) 控制策略 A(Attribution)。是主体对客体的访问规则集，即属性集合。访问策略实际上体现了一种授权行为，也就是客户对主体的权限允许。

2. 访问控制作用

访问控制的主要作用是，保证合法用户访问受权保护的网络资源，防止非法的主体进入受保护的网络资源，并防止合法用户对受保护的网络资源进行非授权的访问。

访问控制组件包括了 4 个部分：发起者(initiator)、访问控制执行功能(Access Control Enforcement Function，AEF)、访问控制决策功能(Access Control Decision，ADF)以及目标(target)。如图 5-4 所示，发起者是指信息系统中系统资源的使用者，是访问控制系统中的主体。目标是指被发起者访问或试图访问的基于计算机或通信的实体，是访问控制系统中的客体。AEF 的功能是负责建立起发起者与目标之间的通信桥梁，它必须按照 ADF 的授权

查询指示来实施上述动作。即当发起者对目标提出执行操作要求时，AEF 会将这个请求信息通知 ADF，并由 ADF 作出是否允许访问的判断。在信息系统中，ADF 是访问控制的核心。当 ADF 对发起者提出的访问请求进行判断时，所依据的是一套访问控制策略和上下文信息。

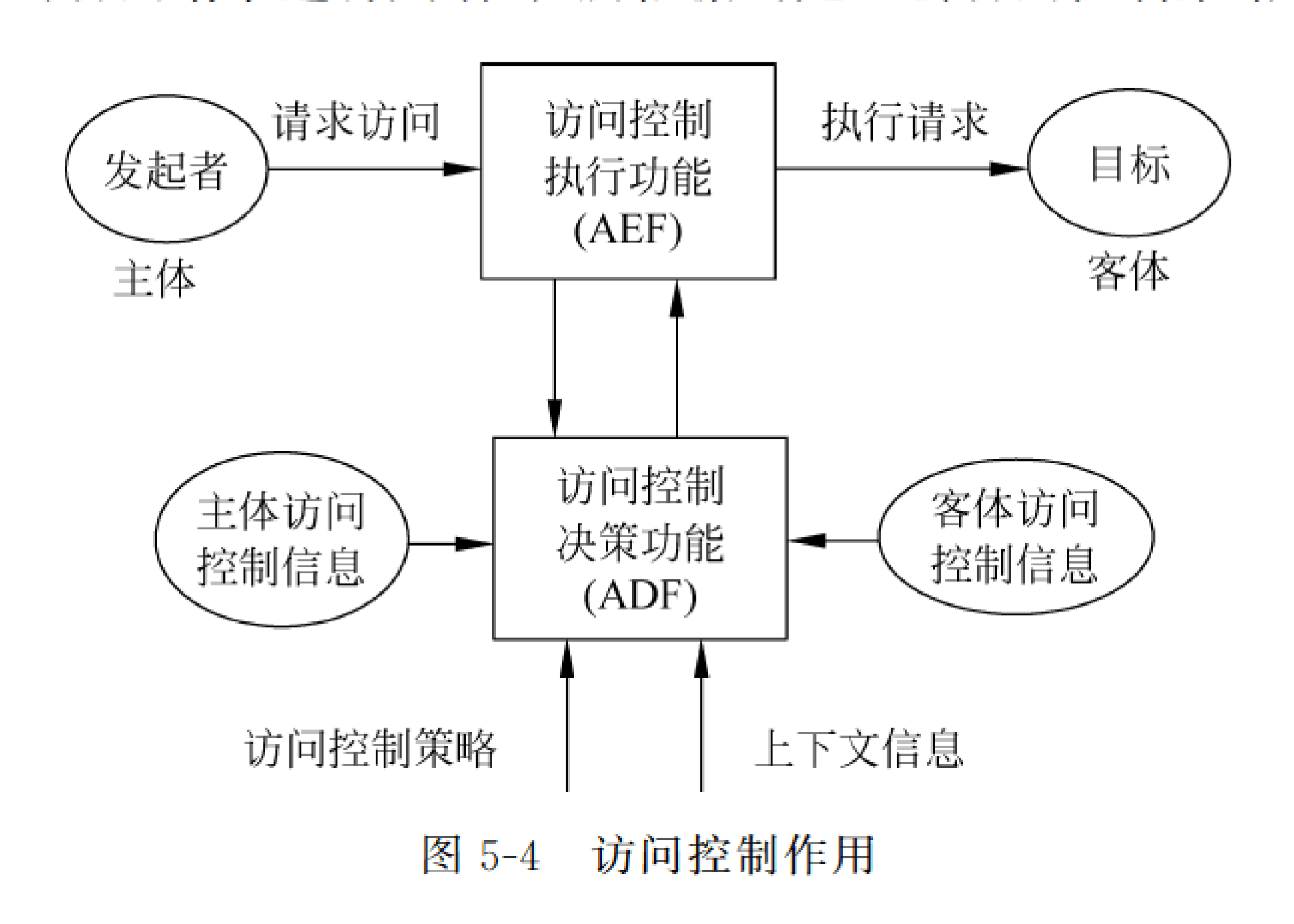


图 5-4　访问控制作用

3. 访问控制模式

主要的访问控制模式有三种，即自主访问控制、强制访问控制和基于角色的访问控制。

(1) 自主访问控制(Discretionary Access Control，DAC)。指资源的所有者决定是否允许特定的人访问资源，类似于目前大多数企业系统管理采取的做法。这种访问控制模式的有效性依赖于资源的所有者对企业安全政策的正确理解和有效落实。

(2) 强制访问控制(Mandatory Access Control，MAC)。指定义几个特定的信息安全级别，将资源归属于这些安全级别中。主体的权限取决于其访问许可等级。

(3) 基于角色的访问控制(Role-Based Access Control，RBAC)。指主体基于特定的角色访问客体，操作权限定义在角色当中。

5.2.2　自主访问控制

自主访问控制最早出现在 20 世纪 70 年代初期的分时系统中，它是多用户环境下最常用的一种访问控制技术，也是目前计算机系统中实现最多的访问控制机制。在自主访问控制的机制下，客体的拥有者全权管理有关该客体的访问授权，有权泄露、修改该客体的有关信息。也就是说，允许某个主体显式地指定其他主体对该主体所拥有的信息资源是否可以访问以及可执行的访问类型。因此自主访问控制又被称为基于拥有者的访问控制。

自主访问控制一般采用访问控制矩阵、访问控制列表和访问控制能力列表三种机制来存放不同主体的访问控制权限，从而完成对主体访问权限的限制。

实现自主访问控制最直接的方法是利用访问控制矩阵。访问控制矩阵的每一行表示一个主体，每一列表示一个受保护的客体，矩阵中的元素表示主体可对客体进行的访问模式(例如读、写、执行、修改、删除等)。

表 5-2 是一个自主访问控制矩阵的示例，表中的 John、Alice、Bob 是三个主体，客体有 4 个文件和两个账户。需要指出的是，Own 的确切含义可能因不同的系统而异，通常一个文件的 Own 权限可以授予或者撤销其他用户对该文件的访问控制权限。例如 John 拥有文件 1 的 Own 权限，他就可以授予 Alice 读或者 Bob 读、写的权限，也可以撤销赋给他们的权限。

表 5-2 访问控制矩阵示例

	文件 1	文件 2	文件 3	文件 4	账户 1	账户 2
John	Own R W		Own R W		Inquiry Credit	
Alice	R	Own R W	W	R	Inquiry Debit	Inquiry Credit
Bob	R W	R		Own R W		Inquiry Debit

访问控制矩阵虽然直观,但是我们可以发现并不是每个主体和客体之间都存在着权限关系。相反,实际的系统中虽然可能有很多的主体和客体,但主体和客体之间的权限关系可能并不多,这样就存在着很多的空白项。因此在实现自主访问控制时,因为将矩阵整体地保存起来效率会很低,所以通常不这么做。实际的方法是基于矩阵的行(主体)或列(客体)来表示访问控制信息。

1. 基于行的自主访问控制

基于行的自主访问控制是在每个主体上都附加一个该主体可访问的客体的列表。根据列表的内容不同,又有不同的实现方式。主要利用能力表(capability list)、前缀表(profiles list)和口令(password)来实现。其中最常用的方法是利用能力表实现。能力决定用户是否可以对客体进行访问以及进行何种模式的访问,拥有相应能力的主体可以以给定的模式访问客体。

如图 5-5 所示,在访问控制能力表中,由于它着眼于某一主体的访问权限,以主体为出

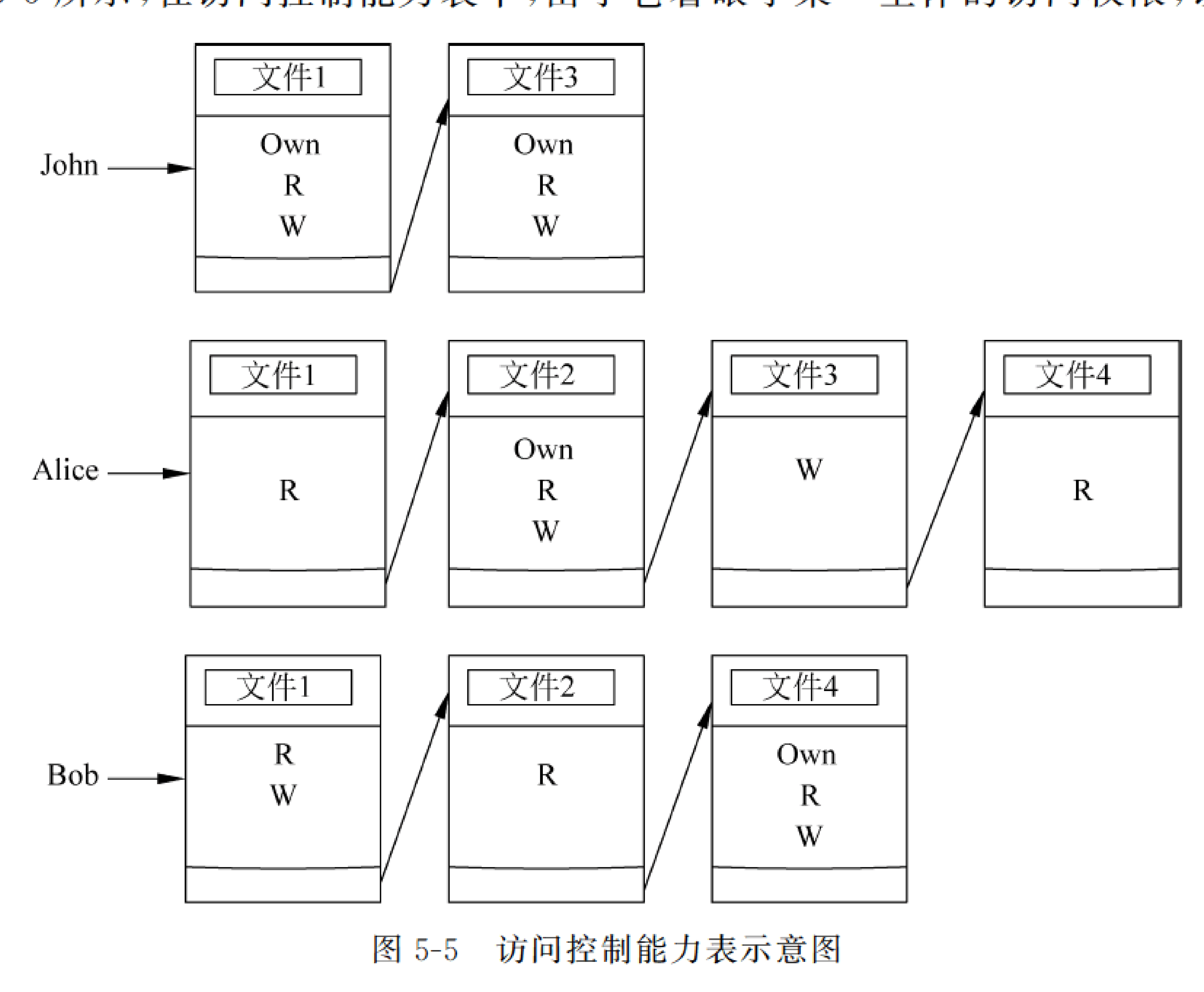


图 5-5 访问控制能力表示意图

发点描述控制信息，因此很容易获得一个被主体授权可以访问的客体及其权限，但是如果要求获得对于某一特定权限的所有主体会比较困难。而且当一个客体被删除之后，系统必须在每个客户的表上清除该客体相应的条目。

2. 基于列的自主访问控制

在基于列的自主访问控制中，每个客体都附加一个可访问它的主体明细表。基于列的自主访问控制最常用的实现方式是访问控制列表。

访问控制列表（Access Control List，ACL）是实现基于列的自主访问控制采用最多的一种方式。它可以对某一特定资源指定任意一个用户的访问权限，还可以将有相同权限的用户分组，并授予组的访问权。图 5-6 所示为访问控制列表的示例。

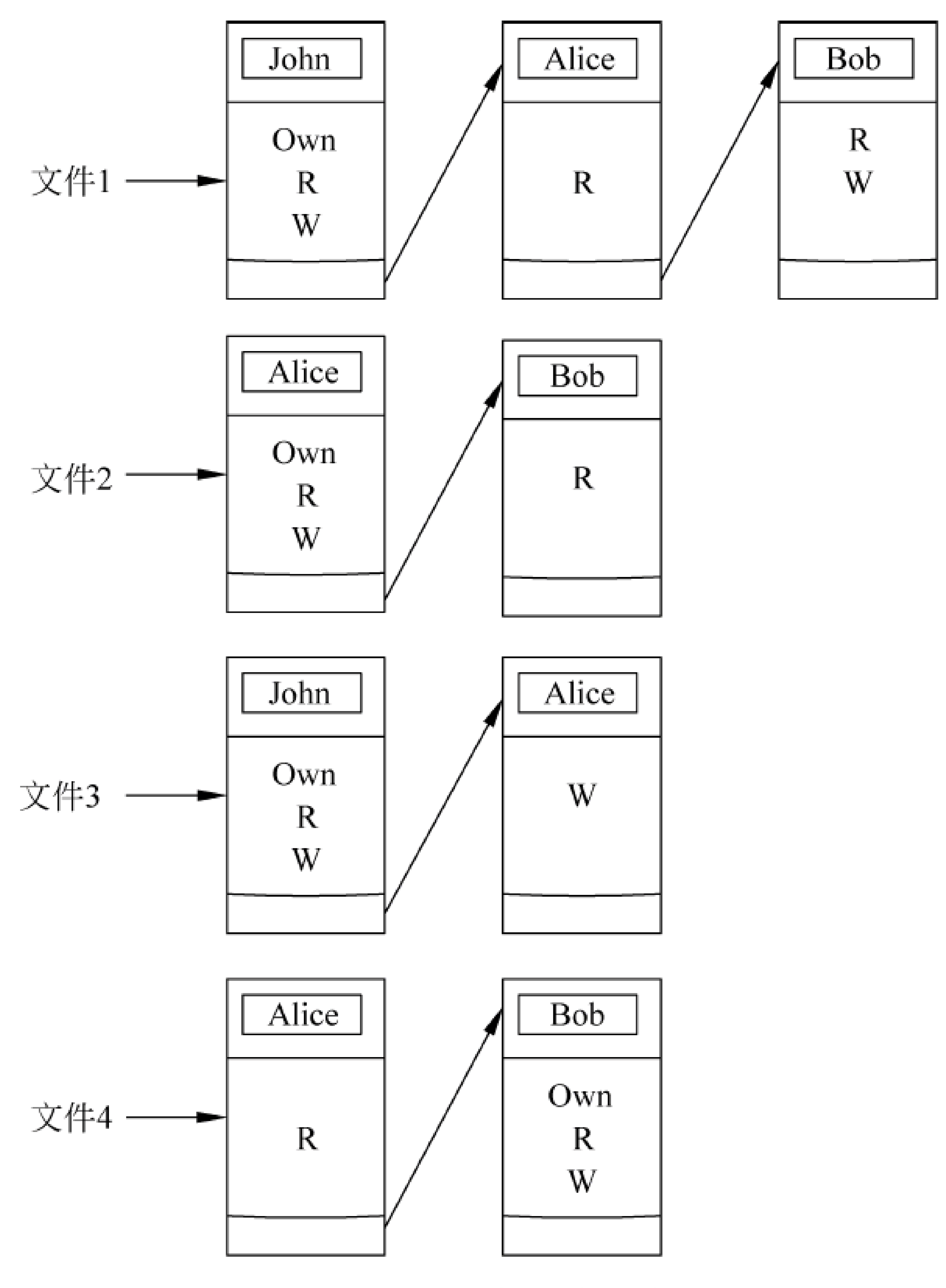


图 5-6　访问控制列表示意图

ACL 的优点在于表述直观，易于理解，而且比较容易查出对某一特定资源拥有访问权限的所有用户，可以有效地实施授权管理。在一些实际应用中，还对 ACL 做了扩展，从而进一步控制用户的合法访问时间，决定是否需要审计等。

尽管 ACL 灵活方便，但将它应用到网络规模较大、需求复杂的企业内部网络时，ACL 需对每个资源指定可以访问的用户或组以及相应的权限。当网络中资源很多时，需要在 ACL 中设定大量的表项。当用户的职位、职责发生变化时，为反映这些变化，管理员需要修改用户对所有资源的访问权限。另外，在许多组织中，服务器一般是彼此独立的，各自设置自己的 ACL。为了实现整个组织范围内的一致的控制策略，需要各管理部门的密切合作。所有这些使得访问控制的授权管理变得费力而烦琐，且容易出错。

上述两种自主访问控制方法都存在一些局限性，主要体现在：资源管理比较分散；用户间的关系不能在系统中体现出来，不易管理；信息容易泄露，无法抵御特洛伊木马的攻击。在自主访问控制下，一旦带有特洛伊木马的应用程序被激活，特洛伊木马可以任意泄露和破坏接触到的信息，甚至改变这些信息的访问控制模式。

在自主访问控制系统中，一个拥有一定访问权限的主体可以直接或间接地将权限传给其他主体。管理员难以确定哪些用户对哪些资源有访问权限，不利于实现统一的全局访问控制。另外，在许多组织中，用户对自己所能访问的资源并不具有所有权，组织本身才是系统中资源的真正所有者。各组织一般希望访问控制与授权机制的实现结果能与组织内部的规章制度相一致，并且由管理部门统一实施访问控制，不允许用户自主地处理，显然，自主访问控制已不能适应这些需求。

5.2.3 强制访问控制

顾名思义，强制访问控制是“强加”给访问主体的，即系统强制主体服从访问控制策略。

强制访问控制的基本思想是：每个主体都有既定的安全属性，每个客体也都有既定安全属性，主体对客体是否能执行特定的操作，取决于二者安全属性之间的关系。这些安全属性是不能改变的，它是由管理部门（如安全管理员）自动地按照严格的规则来设置，不像访问控制列表那样可以由用户直接或间接地修改。当主体对客体进行访问时，根据主体的安全属性和访问方式，比较主体的安全属性和客体的安全属性，从而决定是否允许主体的访问请求。主体不能改变自身的或任何客体的安全属性，包括不能改变属于用户的客体的安全属性，而且主体也不能将自己拥有的访问权限授予其他主体。

强制访问控制和自主访问控制是两种不同类型的访问控制机制，它们常结合起来使用。仅当主体能够同时通过自主访问控制和强制访问控制检查时，它才能访问一个客体。利用自主访问控制，用户可以有效地保护自己的资源，防止其他用户的非法获取；而利用强制访问控制可提供更强有力的安全保护，使用户不能通过意外事件和有意识的误操作逃避安全控制。强制访问控制特别适用于多层次安全级别的军事应用，也适用于政府部门、金融部门等。

安全级由以下两方面的内容构成。

（1）保密级别：又叫敏感级别，可以分为绝密级、机密级、秘密级、无密级等。

（2）范畴集：指在组织系统中，根据人员的不同职能所划分的不同领域。如人事处、财务处等。

安全级包括一个保密级别和任意多个范畴。安全级通常写成保密级别后跟随一个范畴集的形式，如{机密：人事处，财务处}；范畴集可以为空。

在安全级中保密级别是线性排列的，例如，无密＜秘密＜机密＜绝密；范畴集则是互相独立和无序的，两个范畴集之间的关系是包含、被包含或无关。

强制访问控制最主要的优势在于它有阻止特洛伊木马的能力。特洛伊木马是在执行某些合法功能的程序中隐藏的代码，它利用运行此程序的主体的权限违反安全策略，通过伪装成有用的程序在进程中泄露信息。

阻止特洛伊木马的策略是基于非循环信息流，所以在一个级别上读信息的主体一定不能在另一个违反非循环规则的安全级别上写信息。所谓上读，指的是低级别的用户能够读高敏感度区域，下读指低级别用户只能读更低级别的敏感信息，不能读高级别敏感信息。所

谓上写，指的是不允许高敏感的信息写入低敏感区域，下写则允许高敏感度的信息写入低敏感区域。一般用上读/下写来保证数据完整性及利用下读/上写来保证数据的机密性，同样，在一个安全级别上写信息的主体也一定不能在另一个违反非循环规则的安全级别上读信息。由于强制访问控制策略是通过梯度安全标签实现信息的单向流通，所以它可以很好地阻止特洛伊木马的泄密。

强制访问控制的主要缺陷在于实现工作量太大，不够灵活。而且强制访问控制过于偏重保密性，对其他方面如系统连续工作能力、授权的可管理性等考虑不足。

5.2.4 基于角色的访问控制

随着网络技术的发展，网络应用系统所面临的一个难题就是如何对日益复杂的数据资源进行安全管理。传统的访问控制技术都是由主体和访问权限直接发生关系，在实际应用中，当主体和客体的数目都非常大时，传统访问控制技术已远远不能胜任复杂的授权管理的要求。

目前，大部分信息资源服务器对信息没有进行统一管理，特别是没有根据信息的安全要求来进行管理。有些资源服务器虽然采取了一些诸如身份认证、访问控制等安全策略，但由于管理的力度太弱，无法做到对资源的全面控制。还有些资源服务器根据信息的秘密程度分为未知、普通、秘密、机密、绝密 5 级，然后给用户赋予访问权限，这种方式在一定程度上能解决信息的非授权访问问题，但这种方式往往会出现为用户分配的权限比它实际应该具有的权限要大的情况，即没有实现最小特权机制。这些问题都给信息资源的安全留下了重大隐患。

近年来，为了满足新的安全需求，各国学者对访问控制技术进行了大量研究。一方面，对传统访问控制技术的不足进行改进；另一方面，研究新的访问控制技术以适应当前计算机信息系统的安全需求，从而产生了一些更为灵活的访问控制技术。其中，基于角色的访问控制的应用最为广泛。RBAC 的概念早在 20 世纪 90 年代就已经提出，但在相当长的一段时间内没有得到人们的重视。进入 20 世纪 90 年代，安全需求的发展使得 RBAC 又引起人们极大的关注。目前美国的很多学者和研究机构都在从事这方面的研究，NIST（National Institute of Standard Technology）的研究人员认为 RBAC 将成为 DAC 和 MAC 的替代者。

RBAC 的核心思想是将访问权限与角色相联系，通过给用户分配合适的角色，让用户与访问权限相关联。角色是根据企业内为完成各种不同的任务需要而设置的，根据用户在企业中的职权和责任来设定他们的角色。用户可以在角色间进行转换，系统可以添加、删除角色，还可以对角色的权限进行添加、删除。通过应用 RBAC，可以将安全性放在一个接近组织结构的自然层面上进行管理。因此，在 RBAC 中，可以根据组织结构中不同的职能岗位划分角色，资源访问权限被封装在角色中，用户通过赋予的角色间接地访问系统资源，并可对系统资源进行许可范围内的操作。

如图 5-7 所示，RBAC 包含三个实体：用户（user）、角色（role）和权限（privilege）。

用户是对数据对象进行操作的主体，可以是人或计算机等。权限表示对系统中客体进行特定模式访问的操作许可，即对某一数据对象的可操作权利。对数据库系统而言，数据对象可以是表、视图、字段、记录，相应的操作有读、插入、删除和修改等。一项许可就是可以对某一个数据对象进行某一种特定操作的权利。

在 RBAC 中，角色对应于组织中某一特定的职能岗位，具有处理某些事物的许可。这与实际生活中的角色很相似，以学校为例，角色可以是校长、处长、科长、教师、学生等，不过

在 RBAC 中的角色与实际的角色概念有所不同。在一个 RBAC 模型中，一个用户可以被赋予多个角色，一个角色也可以对应多个用户，这些角色是根据系统的具体实现来定义的。同样的一个角色可以拥有多个权限，一个权限也可以被多个用户所拥有。这样在权限管理中，角色作为中间桥梁把用户和权限联系起来，一个角色与若干个权限关联可以看作是该角色拥有的一组权限集合，与用户关联也可以看作是若干具有相同身份的用户集合。

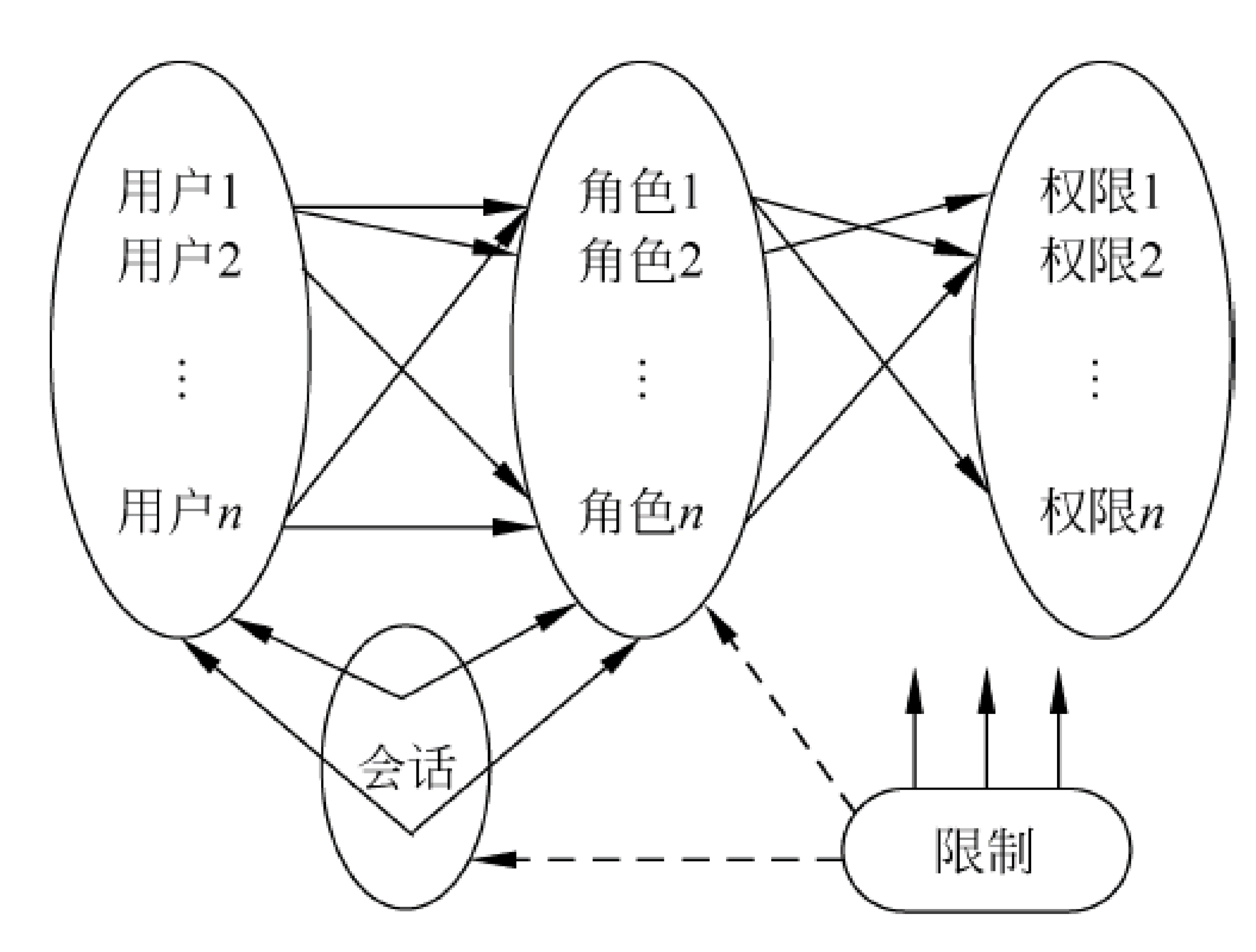


图 5-7　用户、角色和权限的关系图

会话是一个动态的概念，一次会话是用户的一个活跃进程，代表用户与系统进行的一次交互。用户与会话是一对多关系，一个用户可同时打开多个会话。在 RBAC 中，在用户和访问权限之间引入角色的概念。用户与特定的一个或多个角色相联系，角色与一个或多个权限相联系，角色可以根据实际的工作需要生成或取消，而且登录到系统中的用户可根据自己的需要动态激活自己拥有的角色，从而避免用户无意中危害系统安全。除此之外，角色之间、权限之间、角色和权限之间定义了一些关系，如角色间的层次性关系，而且也可以按需要定义各种约束，如定义出纳和会计这两个角色为互斥角色(即这两个不能分配给一个用户)。

从图 5-7 中，我们不难理解角色之间有重叠，如果将重叠部分设置为一个角色 R，其他角色既包含该角色 R 也包含自己的私有部分，这样就产生了角色层次。例如，处长的权限包括了他所主管的各科长的权限，科长的权限包括了其属下各科员的权限。

约束是施加于单个角色之上或多个角色之间的，用来表达权限的执行是有条件的。最常见的约束有基数约束即可被赋予某特定角色的用户数目的约束；或者是用户分配阶段有些权限不能同时被同一个用户获得的静态责任互斥。

用户所执行的操作与其所扮演的角色的职能相匹配，这正是 RBAC 的根本特征。即依据 RABC 策略，系统定义了各种角色，每种角色可以完成一定的职能。不同的用户根据其职能和责任被赋予相应的角色，一旦某个用户成为某角色的成员，则此用户可以完成该角色所具有的职能。

角色由系统管理员定义，角色成员的增减也只能由系统管理员来执行，即只有系统管理员有权定义和分配角色。用户与客体之间无直接联系，他只有通过角色才能享有该角色所对应的权限，从而访问相应的客体，因此用户不能自主地将访问权限授予别的用户，这是 RBAC 与 DAC 的根本区别所在。RBAC 与 MAC 的区别在于，MAC 是基于多级安全需求的，而 RBAC 不是，因为军用系统中主要关心的是防止信息从高安全级流向低安全级，重点考虑的是信息的机密性，而基于角色控制的系统中主要关心的是保护信息的完整性。

综上所述,RBAC 具有以下特点。

(1) 以角色作为访问控制的主体。用户以什么样的角色对资源进行访问,决定了用户拥有的权限以及可执行何种操作。RBAC 的基本思想是:授权给用户的访问权限通常由用户在一个组织中担当的角色来确定。传统的访问控制是将主体和受控客体直接相联系,而 RBAC 在主体与客体之间加入了角色,通过角色沟通主体与客体。这样分层的优点是当主体发生变化时,只需修改主体与角色之间的关联,而不必修改角色与客体的关联。

(2) 角色继承。RBAC 中利用角色之间的层次关系提高授权效率,避免相同权限的重复设置。RBAC 采用了"角色继承"的概念,角色继承是指角色不仅具有直接为其分配的权限,还可以继承其他角色的权限。角色继承把角色组织起来,能够很自然地反映组织内部人员之间的职权、责任关系。

角色继承可以用父子关系来表示。如图 5-8 所示,角色 2 是角色 1 的"父亲",它包含角色 1 的属性与权限。在角色继承关系图中,处于最上面的角色拥有最大的访问权限,越下端的角色拥有的权限越小。

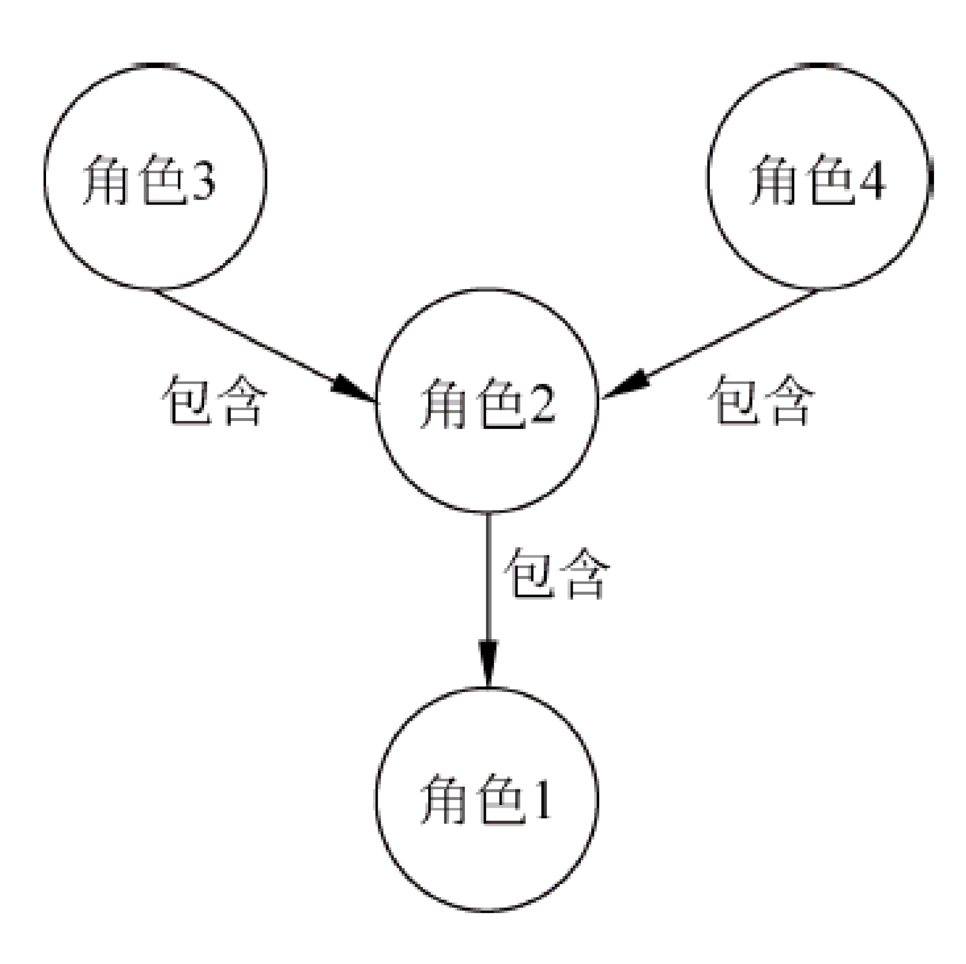


图 5-8　角色的继承关系示意图

(3) 最小特权原则。所谓最小特权原则(least privilege policy)是:用户所拥有的权力不能超过他执行工作时所需的权限。实现最小特权原则,需分清用户的工作内容,确定执行该项工作的最小权限,然后将用户限制在这些权限范围之内。在 RBAC 中,可以根据组织内的规章制度、职员的分工等设计拥有不同权限的角色,只有角色需要执行的操作才授予给角色。当一个主体准备访问资源时,如果该操作不在主体当前活跃角色的授权操作之内,该访问将被拒绝,由此体现了最小特权原则。

5.3　数字签名技术

5.3.1　数字签名概述

在实际网络通信中,用户可能受到来自多方面的攻击。在现实环境中,可以通过当面交易的方式或者通过手写签名盖章的方式来解决通信双方的欺骗和抵赖行为。但在网络环境中,每个人都是虚拟的,如何能够实现同现实中手写签名类似的功能?这就是数字签名要解决的问题,在了解数字签名概念之前,先看下面的例子。

用户 A 与 B 相互之间要进行通信,双方拥有共享的会话密钥 K,在通信过程中可能会遇到以下问题:

A 伪造一条信息,并称该消息来自于 B。A 只需要产生一条伪造的消息,用 A 和 B 的共享密钥通过哈希算法产生认证码,并将认证码附于消息之后。由于哈希算法的单向性和密钥 K 是共享的,因此无法证明该消息是 A 伪造的。

B 可以否认曾经发送过某条消息。因为任何人都有办法伪造消息,所以无法证明 B 是否发送过该消息。

上述例子说明使用哈希算法可以进行报文鉴别,但无法阻止通信用户的欺骗和抵赖行

为。因此，当通信双方不能相互信任的情况下，需要用除了报文鉴别以外的技术来防止类似的抵赖和欺骗行为。

1. 数字签名概念

数字签名(Digital Signature)指用户用私钥对原始数据加密所得的特殊数字串，用于保证信息来源的真实性、数据传输的完整性和防抵赖性。数字签名在电子银行、证券和电子商务等方面应用非常广泛，如汇款、转账、订货、票据、股票成交等。用户以电子邮件等方式，使用个人私有密钥加密数据或选项后，发送给接收者。接收者用发送者的公钥解开数据后，就可确定数据源。数字签名同时也是对发送者发送信息真实性的证明，发送者对所发送的信息不可抵赖。

2. 数字签名功能

(1) 签名是可信的。文件的接收者相信签名者是慎重地在文件上签名的。

(2) 签名是不可抵赖的。发送者事后不能抵赖对报文的签名，可以核实。

(3) 签名不可伪造。可以证明是签字者而不是其他人在文件上签字。

(4) 签名不可重用。签名是文件的一部分，不可将签名移动到其他的文件。

(5) 签名不可变更。签名和文件不能改变，也不可分离。

(6) 数字签名有一定的处理速度，能够满足所有的应用需求。

3. 数字签名种类

1) 手写签名或印章的识别

将手写签名或印章作为图像，用光扫描经光电转换后在数据库中加以存储。当验证手写签名或印章时，也用光扫描输入，并将原数据库中的对应图像调出，用模式识别的数学计算方法对两者进行比对，以确认该签名或印章的真伪。这种方法曾经在银行会计柜台使用过，但由于需要大容量的数据库存储，而且每次手写签名和印章存在差异，实用性不强，也不适合在互联网上传输。

2) 生物识别

生物识别技术是利用人体生物特征进行身份认证的一种技术。生物特征是一个人与他人不同的唯一表征，可以测量、自动识别和验证。生物识别系统对生物特征进行取样，提取其唯一的特征进行数字化处理，转换成数字代码，并进一步将这些代码组成特征模板存储在数据库中。人们同识别系统交互进行身份认证时，识别系统获取其特征并与数据库中的特征模板进行比对，以确定是否匹配，从而决定确认或否认此人。生物识别技术主要包括指纹、声音、人像、掌形、视网膜、虹膜、脸型、DNA 和多种方法综合等识别技术。

3) 密码、密码代号或个人识别码

密码、密码代号或个人识别码主要是指用一种传统的对称密钥加/解密的身份识别和签名方法。甲方需要乙方签名一份电子文件，甲方可产生一个随机码传送给乙方，乙方用事先双方约定好的对称密钥加密该随机码和电子文件后回送给甲方，甲方用同样的对称密钥解密后得到电文并核对随机码，如随机码核对正确，甲方即可认为该电文来自乙方。

4) 基于量子力学的计算机

基于量子力学的计算机被称为量子计算机，是以量子力学原理直接进行计算的计算机，比传统的图灵计算机具有更强大的功能，其计算速度比现代的计算机快几亿倍。量子计算机对目前采用的密码技术提出了挑战，它采用一种新的量子密码方式，即利用光子的相位特性编码。传统密码在被窃听者破解时不留下痕迹，但这种密码不同，由于量子力学的随机性

非常特殊，无论多么聪明的窃听者，在破译这种密码时都会留下痕迹，甚至在密码被窃听的同时会自动改变。这将是世界上最安全的密码认证和签名方法，然而，这种量子计算机或光子计算机还只处于研究阶段，没有被广泛应用。

5）基于 PKI 的电子签名

基于 PKI 的电子签名就是数字签名。由于电子签名虽然获得了技术中立性，但使用却不方便，法律上又对电子签名做了进一步规定，如联合国国际贸易法委员会的《电子签名示范法》和欧盟的《电子签名共同框架指令》中就规定了“可靠电子签名”和“高级电子签名”，实际上就是规定了数字签名的功能，这种规定使数字签名获得了更好的应用安全性和操作性。目前，具有实际意义的电子签名只有公钥密码理论，所以目前国内外普遍使用的还是基于 PKI 的数字签名。作为公钥基础设施，PKI 可提供多种网上安全服务，如认证、数据保密性、数据完整性和不可否认性，这些都采用了数据签名技术。

5.3.2 数字签名过程及实现

对一个电子文件进行数字签名并在网上传输，通常需要的技术实现过程包括上网身份认证、进行签名和对签名的认证。

1. 身份认证的实现

PKI 提供的服务首先是认证，即身份识别与鉴别，就是确认实体（用户或所用主机的操作设备或邮箱）即为自己所声明的实体。认证的前提是双方都具有第三方 CA 所签发的证书，认证分为单向认证和双向认证。

1）单向认证

双方在网上通信时，甲只需要认证乙的身份。这时甲需要获取乙的证书。获取证书的方式有两种，一种是在通信时乙直接将证书传给甲，另一种是甲向 CA 的目录服务器查询索取。甲获得乙的证书后，先用 CA 的根证书公钥验证该证书的签名，验证通过说明该证书是第三方 CA 签发的有效证书，然后检查证书的有效期、时效性（LRC 检查）及黑名单。

2）双向认证

双方在网上通信时，双方互相认定身份。其认证过程的各方都与上述单向认证过程相同。双方采用轻量目录访问协议（Lightweight Directory Access Protocol，LDAP）在网上查询对方证书的有效性及黑名单。

2. 数字签名原理

在互相认证身份后，网上通信的双方即可发送签名的数据电文。数字签名过程分为两部分：签名过程和验证过程，如图 5-9 所示。发送方将原文用哈希算法求得数字摘要，用签名私钥对数字摘要加密求得数字签名，然后将原文与数字签名一起发送给接收方。接收方验证签名，即用发送方公钥解密数字签名，得出数字摘要。接收方将原文采用同样的哈希算法又得一个新的数字摘要，将两个数字摘要进行比较，如果两者匹配，说明经数字签名的电子文件传输成功。

3. 数字签名的签名过程

数字签名的签名过程如图 5-10 所示，需要有发送方的签名证书的私钥及其验证公钥。数字签名具体的实际操作过程为：生成被签名的电子文件后，对电子文件用哈希算法做数字摘要，再对数字摘要用签名私钥做非对称加密，即做数字签名；将以上的签名、电子文件原文及签名证书的公钥一起封装，形成签名结果发送给接收方验证。

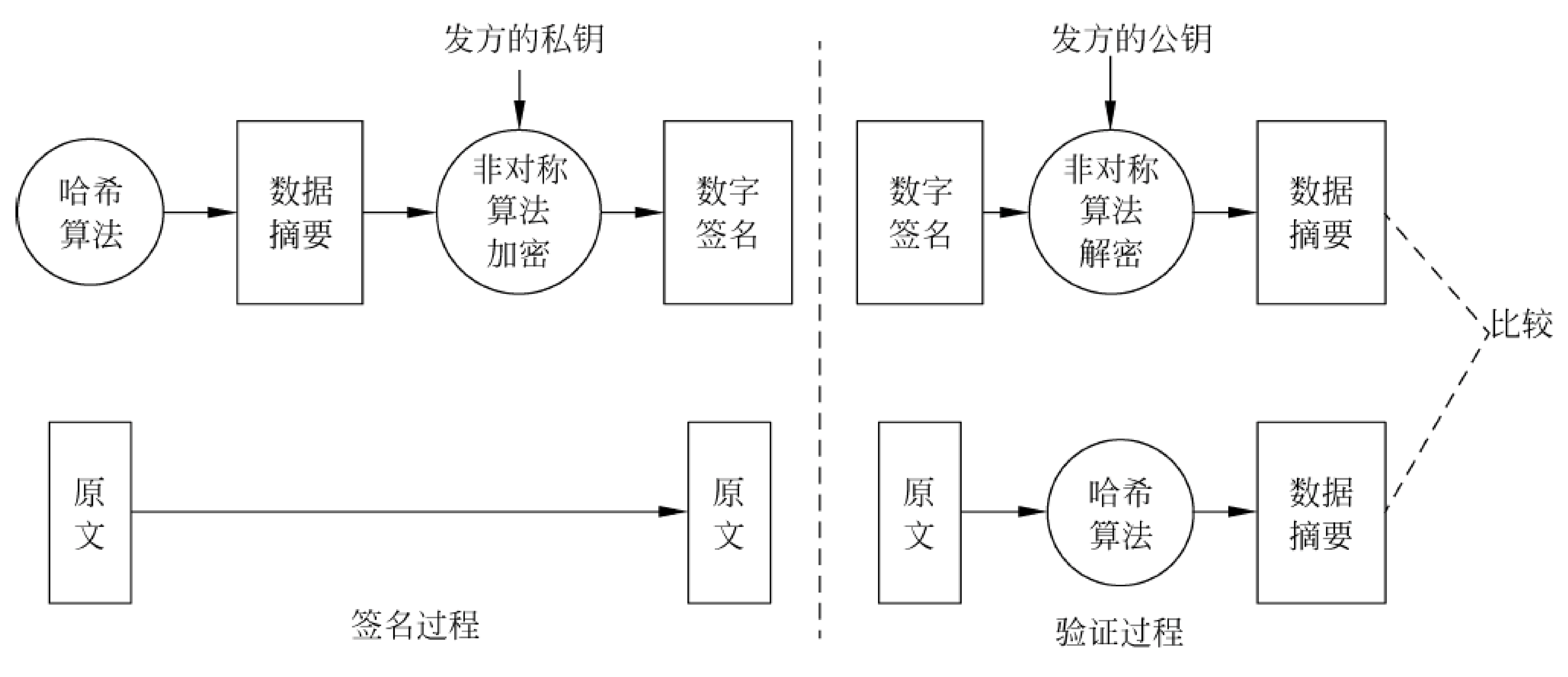


图 5-9　数字签名原理

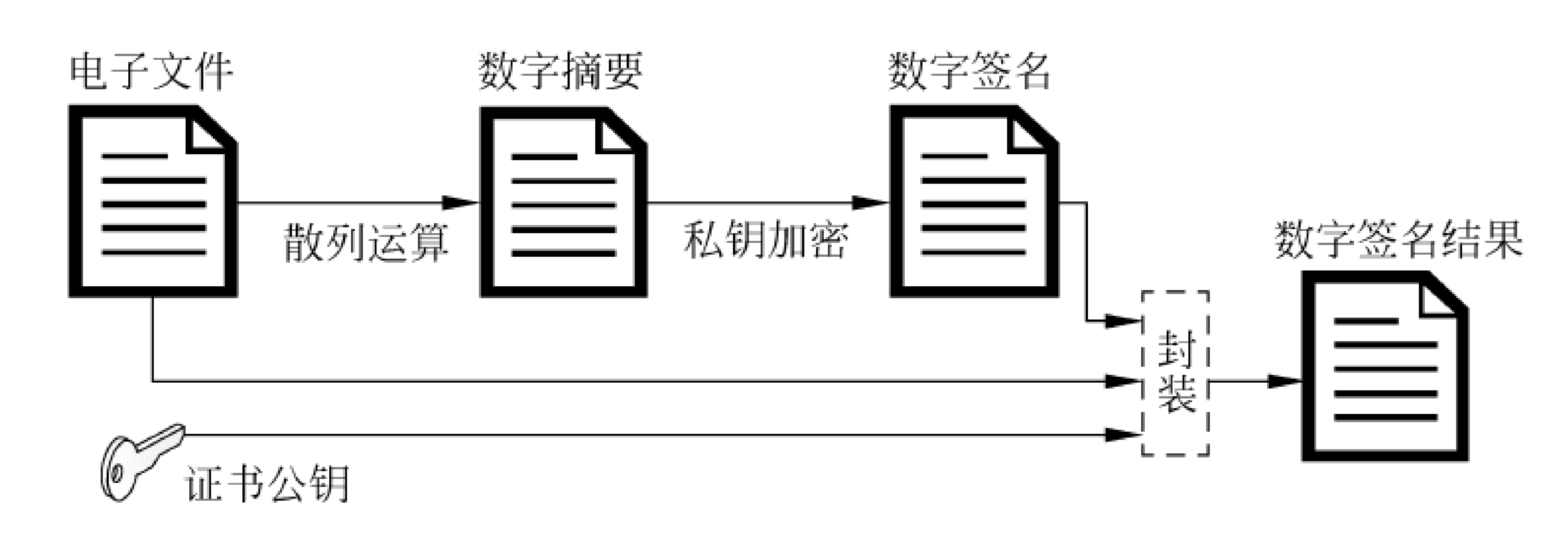


图 5-10　签名过程

4. 数字签名的验证过程

接收方收到发送方的签名后进行签名验证，其具体操作过程如图 5-11 所示，接收方收到数字签名的结果，即待验证的数据，包括数字签名、电子原文和发方公钥。然后，接收方用发送方公钥解密数字签名，导出数字摘要，并对电子文件原文做同样的哈希算法得到一个新的数字摘要，将两个摘要的散列值进行比较，若结果相同则说明签名得到验证，否则签名无效。

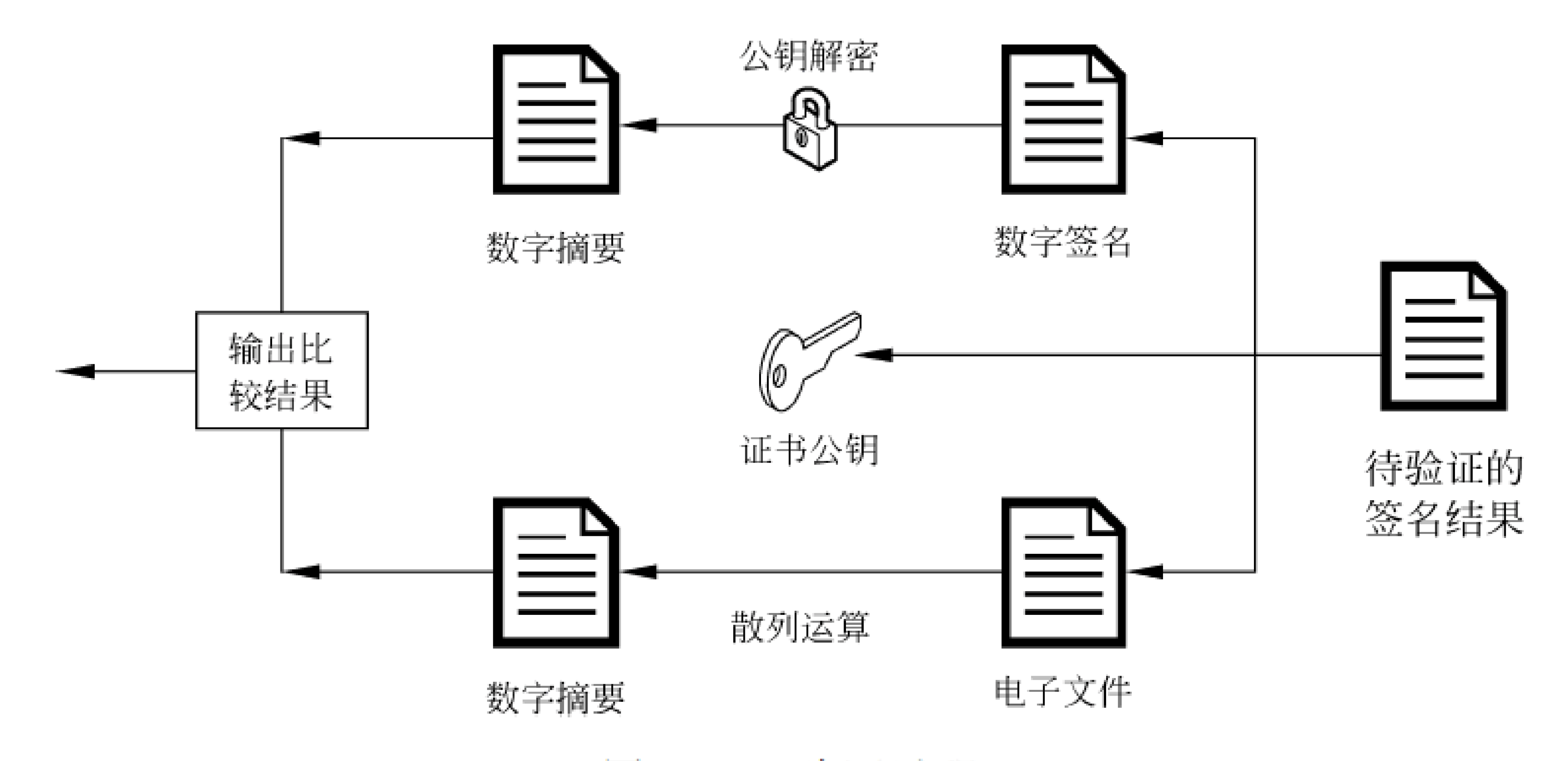


图 5-11　验证过程

如果接收方对发送方的数字签名验证成功，就可以说明三个实质性的问题。

(1) 该电子文件确实是由签名者的发送方所发出的，电子文件来源于该发送者，因为签署时电子签名数据由电子签名人所控制。

（2）被签名的电子文件确实是经发送方签名后发送的，说明发送方用了自己的私钥做的签名，并得到验证，达到不可否认的目的。

（3）接收方收到电子文件在传输中没有被篡改，保持了数据的完整性，因为签署后对电子签名的任何改动都能够被发现。

5. 原文加密的数字签名

原文加密的数字签名的过程要求对数字签名方法的实现涉及“数字信封”的问题，此处理过程稍微复杂一些，但数字签名的基本原理仍相同，其签名过程如图 5-12 所示。

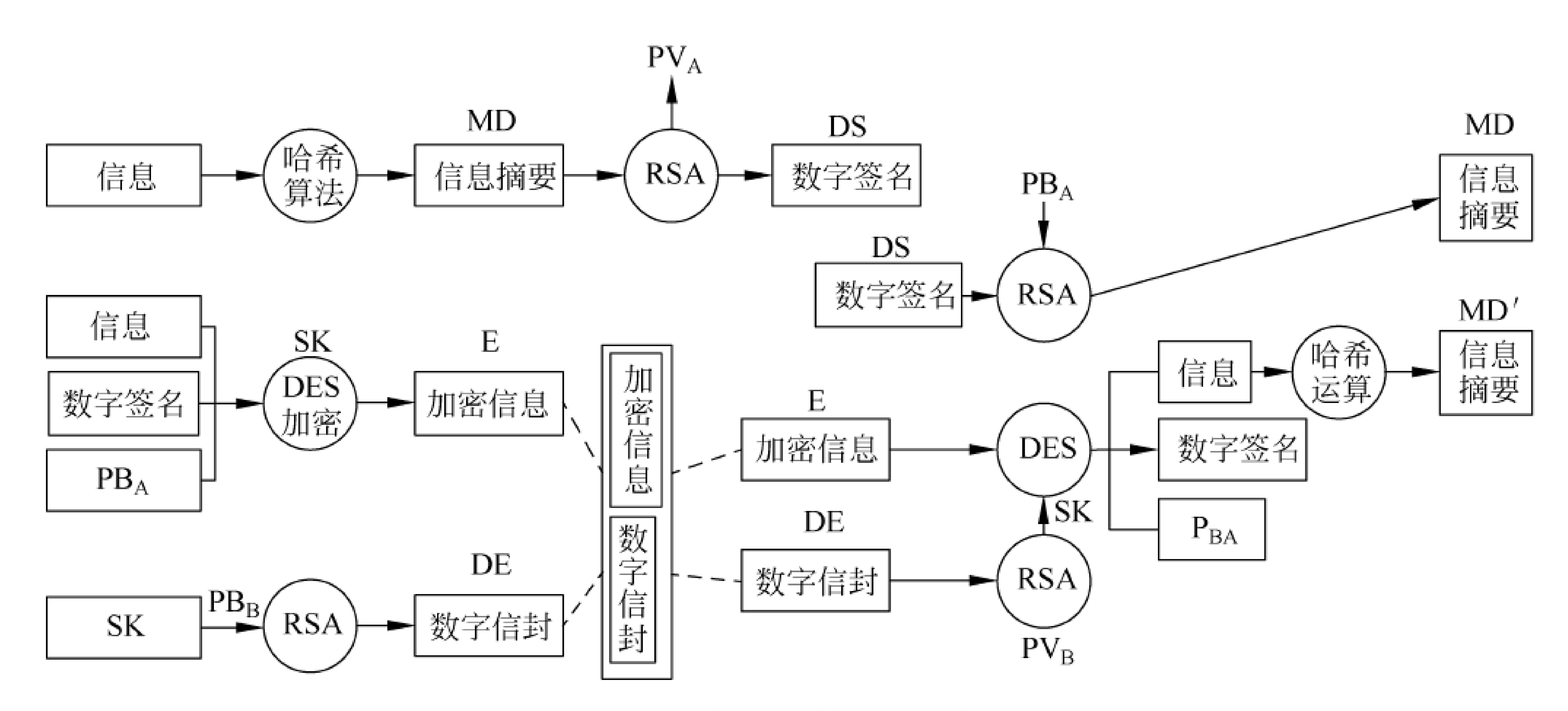


图 5-12 原文加密的数字签名实现方法

这是一个典型的“数字信封”处理过程。其基本原理是将原文用对称密钥加密传输，而将对称密钥用接收公钥加密发送给对方。如同将对称密钥放在同一个数字信封，接收方收到数字信封，用自己的私钥解密信封，取出对称密钥解密原文。

原文加密的数字签名的过程如下。

（1）发送方 A 将原文信息进行哈希算法，得到一哈希值，即数字摘要 MD。

（2）发送方 A 用自己的私钥 PV_A，采用非对称 RSA 算法对数字摘要 MD 加密，即得数字签名 DS。

（3）A 用对称密钥 SK 对原文、数字签名 DS 及 A 证书的公钥 PB_A 加密，得加密信息 E。

（4）发送方用接收方 B 的公钥 PB_B，采用 RSA 算法对对称密钥 SK 加密，形成数字信封 DE，就好像将对称密钥 SK 装到了一个用接收方公钥加密的信封里。

（5）发送方 A 将加密信息 E 和数字信封 DE 一起发送给接收方 B。

（6）接收方 B 接收到数字信封 DE 后，首先用自己的私钥 PV_B 解密数字信封，取出对称密钥 SK。

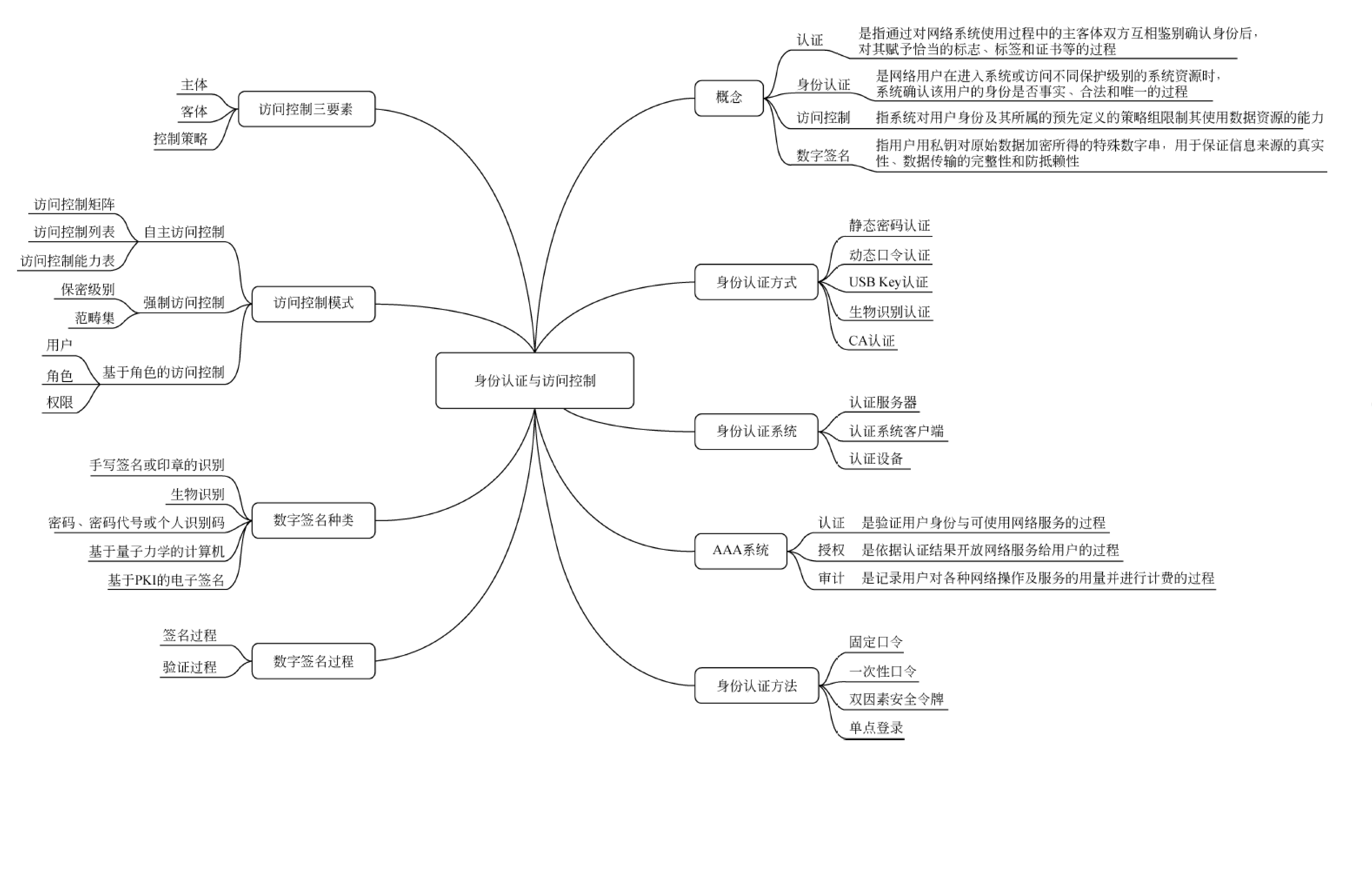
（7）B 用对称密钥 SK 以 DES 算法解密 E 还原出原文、数字签名 DS 及发送方 A 证书的公钥 PB_A。

（8）接收方 B 验证数字签名，先用发送方 A 的公钥解密数字签名得数字摘要 MD。

（9）接收方 B 同时将原文信息用同样的哈希算法，求得一个新的 MD’。

（10）将两个数字摘要 MD 和 MD’进行比较，若相等则说明数据没被篡改，签名真实，否则拒绝该签名。此过程实现了机密信息在数字签名的传输中不被篡改的保密目的。

5.4 本章小结



身份认证与访问控制
概念
认证
是指通过对网络系统使用过程中的主客体双方互相鉴别确认身份后，对其赋予恰当的标志、标签和证书等的过程
身份认证
是网络用户在进入系统或访问不同保护级别的系统资源时，系统确认该用户的身份是否真实、合法和唯一的过程
访问控制
指系统对用户身份及其所属的预先定义的策略组限制其使用数据资源的能力
数字签名
指用户用私钥对原始数据加密所得的特殊数字串，用于保证信息来源的真实性、数据传输的完整性和防抵赖性
身份认证方式
静态密码认证
动态口令认证
USB Key认证
生物识别认证
CA认证
身份认证系统
认证服务器
认证系统客户端
认证设备
AAA系统
认证　是验证用户身份与可使用网络服务的过程
授权　是依据认证结果开放网络服务给用户的过程
审计　是记录用户对各种网络操作及服务的用量并进行计费的过程
身份认证方法
固定口令
一次性口令
双因素安全令牌
单点登录
访问控制三要素
主体
客体
控制策略
访问控制模式
自主访问控制
访问控制矩阵
访问控制列表
访问控制能力表
强制访问控制
保密级别
范畴集
基于角色的访问控制
用户
角色
权限
数字签名种类
手写签名或印章的识别
生物识别
密码、密码代号或个人识别码
基于量子力学的计算机
基于PKI的电子签名
数字签名过程
签名过程
验证过程

5.5 习　　题

一、填空题

1. (　　)认证方式是最简单、应用最广泛的身份认证方法。

2. (　　)是国际认证机构的通称,是对数字证书的申请用户进行发放、管理、校验或取消的机构。

3. AAA 认证系统中(　　)是依据认证结果开放网络服务给用户的过程。

4. (　　)模式是指定义几个特定的信息安全级别,将资源归属于这些安全级别中。

5. 自主访问控制一般采用(　　)、访问控制列表和访问控制能力列表三种机制来存放不同主体的访问控制权限。

二、选择题

1. 数字签名的(　　)功能是指签名可以证明是签名者而不是其他人在文件上签字。

A. 签名不可伪造　　B. 签名不可变更
C. 签名不可抵赖　　D. 签名是可信的

2. (　　)不属于 AAA 系统提供的服务类型。

A. 认证　　B. 授权　　C. 访问　　D. 审计

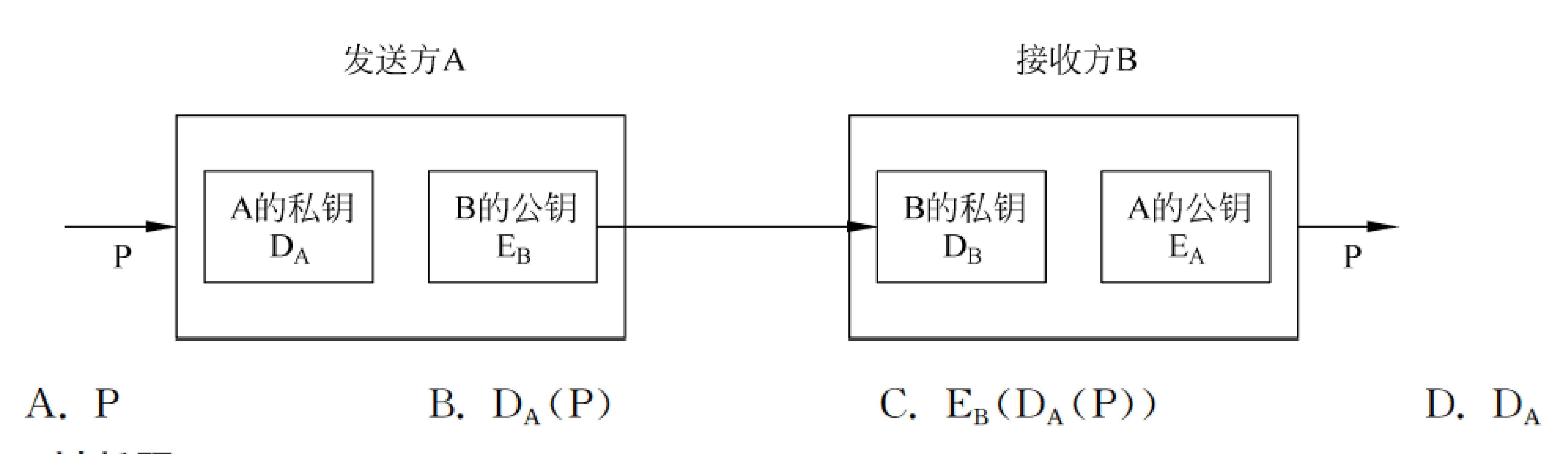
3. PKI 解决信息系统中的(　　)问题。

A. 身份信任　　B. 权限管理　　C. 安全审计　　D. 安全传输

4. 以下关于 CA 认证中心说法正确的是(　　)。

A. CA 认证是使用对称密钥机制的认证方法
B. CA 认证中心只负责签名,不负责证书的产生
C. CA 认证中心负责证书的颁发和管理、并依靠证书证明一个用户的身份
D. CA 认证中心不用保持中立,可以任意找一个用户来作为 CA 认证中心

5. 下图为一种数字签名方案,防止 A 抵赖的证据是(　　)。



A. P　　B. $D_A(P)$　　C. $E_B(D_A(P))$　　D. D_A

三、判断题

1. 基于行的自主访问控制一般采用访问控制能力列表来实现。

2. RBAC 的核心思想就是将访问权限与角色相联系,通过给用户分配合适的角色,让用户与访问权限相关联。

3. 身份认证技术解决了用户是“谁”的问题,访问控制决定了用户“能够做什么”。

4. 访问控制策略是主体对客体的访问规则集,即属性集合。

5. 访问控制列表是实现基于列的自主访问控制采用最多的一种方式。

四、简答题

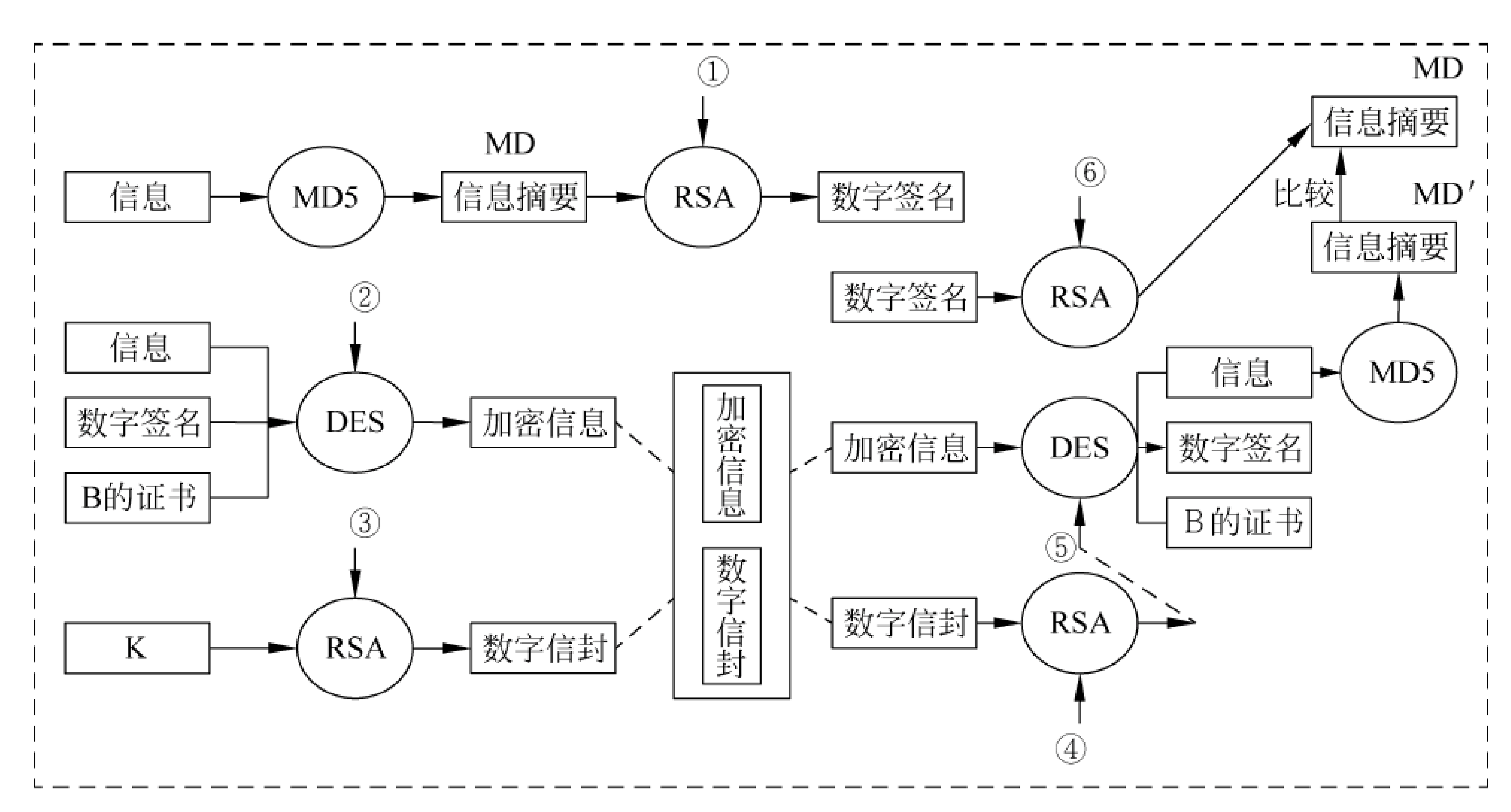
1. 访问控制包括哪三个要素？
2. AAA 系统提供哪些服务？
3. 在实际应用中，数字信封常用来解决什么问题？如何解决？
4. 什么是身份认证？
5. 访问控制模式有哪三种模式？
6. 什么是数字签名？

五、综合题

下图为数字签名工作原理示意图，发送方为 A，接收方为 B。图中①～⑥省略密钥名称。如果对称密钥为 K，发送方私钥为 SA，发送方公钥为 PA，接收方私钥为 SB，接收方公钥为 PB。

(1) 请写出图中①～⑥省略的密钥名称。

(2) 给出接收方比较 MD 和 MD′的目的。



第6章　防火墙技术

【本章学习目标】

- 理解防火墙的概念
- 了解防火墙的功能
- 了解各种防火墙类型
- 掌握包过滤与代理服务技术
- 掌握防火墙的体系结构
- 掌握 PIX 防火墙配置技术

6.1　防火墙概述

6.1.1　防火墙概念

防火墙是由软件和硬件组成的系统，它处于安全的网络(通常是内部局域网)和不安全的网络(通常是因特网，但不局限于因特网)之间，根据系统管理员设置的访问控制规则，对数据流进行过滤。

由于防火墙位于两个网络之间，因此从一个网络到另一个网络的所有数据流都要流经防火墙，根据安全策略，防火墙对数据流的处理方式有三种：①允许数据流通过；②拒绝数据流通过；③将这些数据流丢弃。当数据流被拒绝时，防火墙要向发送者回复一条消息，提示发送者该数据流已被拒绝。当数据流被丢弃时，防火墙不会对这些数据流进行任何处理，也不会向发送者发送任何提示信息。

防火墙一般是指在两个网络间执行访问控制策略的一个或一组系统，如图 6-1 所示。防火墙是架设在用户内部网络和外部公共网络之间的屏障，提供两个网络之间的单点防御，对其中的一个网络(通常是用户内部网络)提供安全保护。其中由防火墙隔离出的空间被称为 DMZ，DMZ 是英文 demilitarized zone 的缩写，中文名称为“隔离区”，也称“非军事化区”。它是一个非安全系统与安全系统之间的缓冲区，用于解决安装防火墙后，外部网络的用户不能访问内部网络服务器的问题。与因特网相比，DMZ 可以提供更高的安全性，但是其安全性比内部网络低。从功能上说，Internet 是不同网络或网络安全域之间信息的唯一出入口，能够根据内部网络的安全策略控制出入网络的信息流，尽可能对外部屏蔽网络内部的信息、结构和运行状况，以防止发生入侵。从逻辑上来说，防火墙是一个分离器、限制器、分析器，它能够有效地监控内部网和外部网之间的所有活动，保证内部网络的安全。从物理上来说，防火墙是位于网络特殊位置的一系列安全部件的组合，它既可以是专用的防火墙硬件设备，

也可以是路由器或交换机上的安全组件，还可以是运行安全软件的主机。

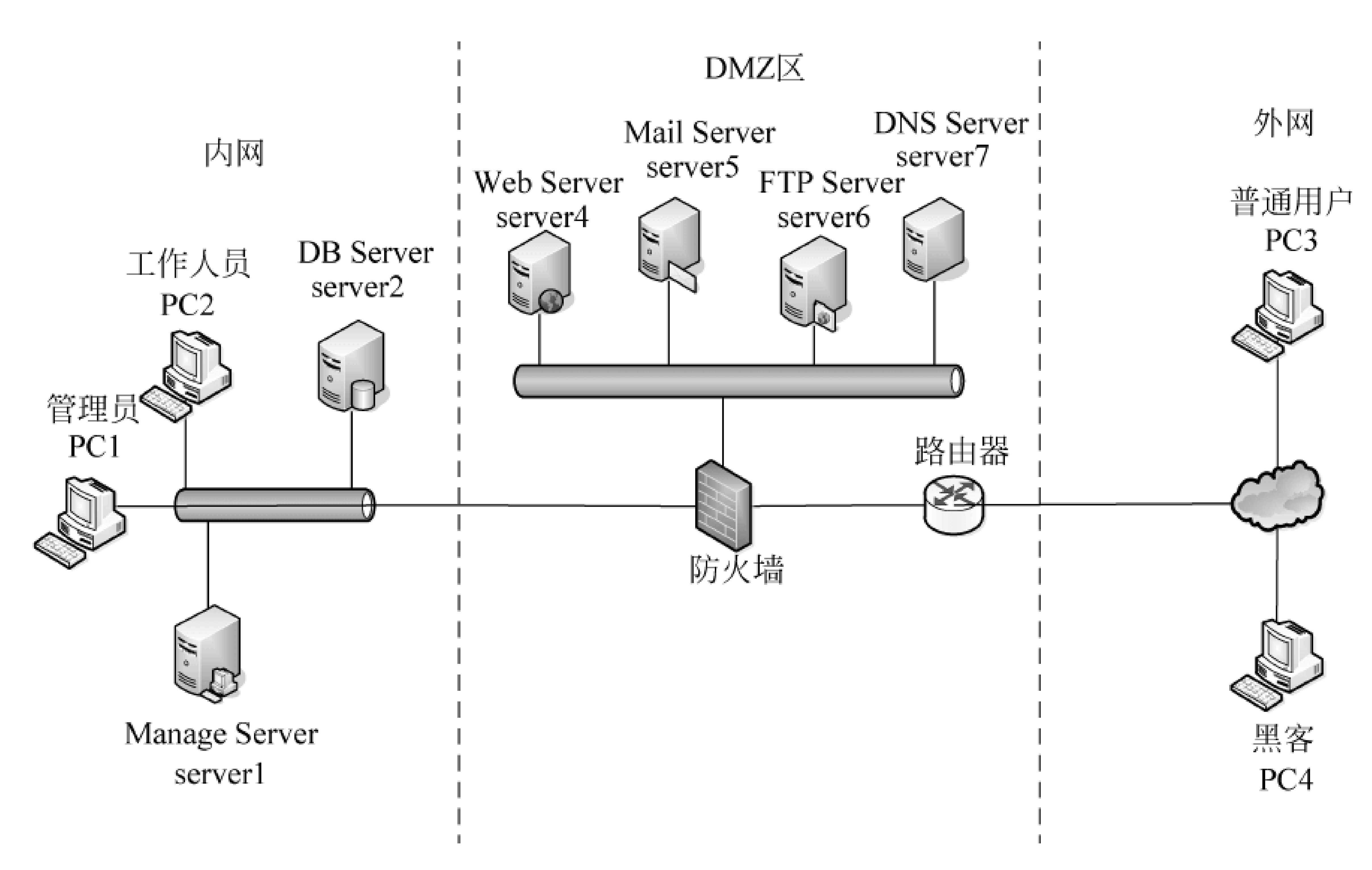


图 6-1　防火墙示意图

6.1.2　防火墙发展

从诞生至今，防火墙经过了几代的发展，现在的防火墙已经与最初的防火墙大不相同了。最初的防火墙依附于路由器，它只是路由器中的一个过滤块。后来随着过滤功能的完善和过滤深度的增加，防火墙逐步从路由器中分离出来，成为一个独立的设备。

迄今为止，防火墙的发展经历了 30 多年的时间。防火墙技术的发展阶段如图 6-2 所示。第一代防火墙始于 1985 年前后，它几乎与路由器同时出现，由 Cisco 的 IOS 软件公司研制。这一代防火墙称为包过滤防火墙。直到 1988 年，DEC 公司的 Jeff Mogul 根据自己的研究，才发表了第一篇描述有关包过滤防火墙过滤过程的文章。

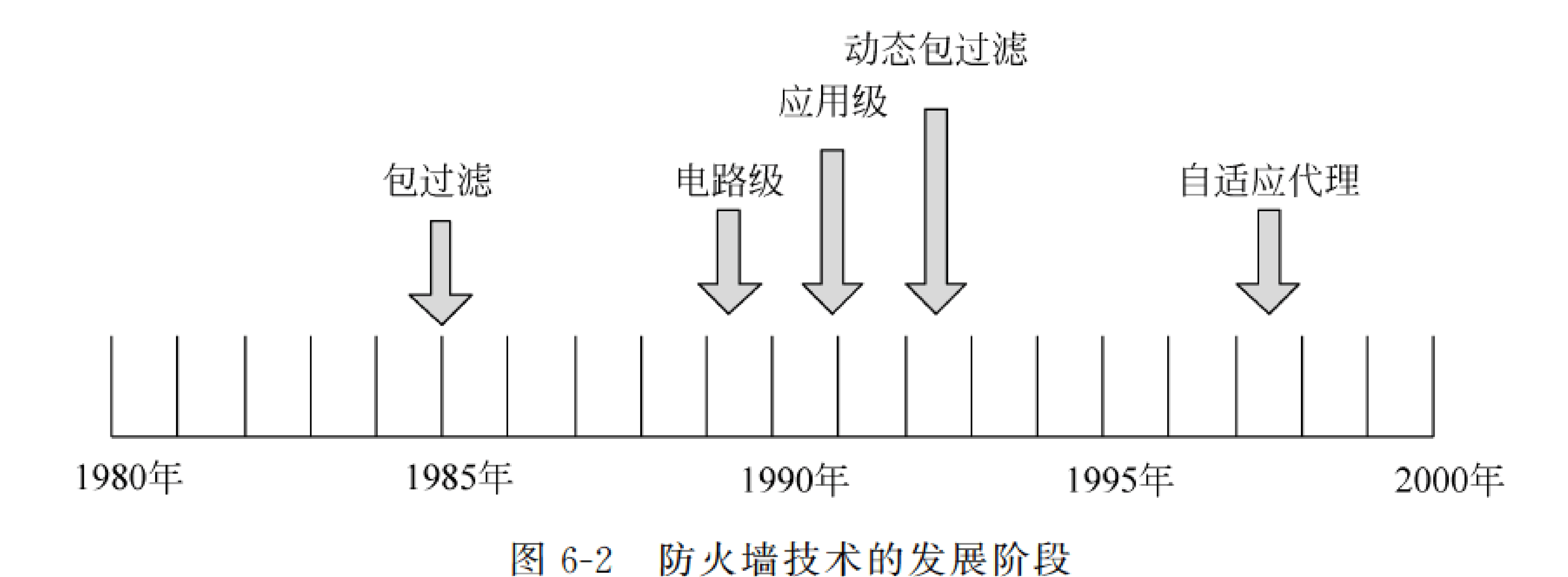


图 6-2　防火墙技术的发展阶段

1989—1990 年前后，AT&T 贝尔实验室的 Dave Presotto 和 Howard Trickey 率先提出了基于电路中继的第二代防火墙结构，此类防火墙被称为电路级网关防火墙。但是，他们既没有发表描述这一结构的任何文章，也没有发布基于这一结构的任何产品。

第三代防火墙结构是在 20 世纪 80 年代末和 20 世纪 90 年代初由普渡大学的 Gene

Spafford、AT&T 贝尔实验室的 Bill Cheswick 和 Marcus Ranum 分别研究和开发的。这一代防火墙被称为应用级网关防火墙。在 1991 年，Ranum 的文章引起了人们的广泛关注。此类防火墙采用了在堡垒主机运行代理服务的结构。根据这一研究成果，DEC 公司推出了第一个商用产品 SEAL。

大约在 1991 年，Bill Cheswick 和 Steve Bellovin 开始了对动态包过滤防火墙的研究。1992 年，在 USC 信息科学学院工作的 Bob Braden 和 Annette DeSchon 开始研究用于 Visas 系统的动态包过滤防火墙，后来它演变为目前的状态检测防火墙。1994 年，以色列的 Check Point Software 公司推出了基于第四代结构的第一个商用产品。

在 1998 年由 NAI 公司推出的自适应代理(Adaptive Proxy)技术给代理类型的防火墙赋予了全新的意义，可以称为第五代防火墙。

6.2 防火墙功能及功能局限性

6.2.1 防火墙功能

防火墙位于网络的边界，因此被认为是边界安全。其主要功能如下。

(1) 建立一个集中的监视点。防火墙位于两个或多个网络之间，对所有流经它的数据包都进行过滤和检查，这些检查点被称为“阻塞点”。通过强制所有进出流量通过阻塞点，网络管理员可以集中管理保障网络安全。

(2) 监视网络的安全性，并产生报警。对一个内部网络已经连接到因特网上的机构来说，重要的问题并不是网络是否会受到攻击，而是何时会受到攻击。网络管理员必须审计并记录所有通过防火墙的重要信息。如果网络管理员不能及时响应报警并审查常规记录，防火墙就形同虚设。

(3) 网络地址转换。网络地址转换是指在局域网内部使用私有 IP 地址，当内部用户要与外部网络进行通信时，就在网络出口处将私有 IP 地址替换成公用 IP 地址。因此，在防火墙上实现网络地址转换，可以缓解 IP 地址空间短缺的问题，并屏蔽内部网络的结构和信息，保证内部网络的稳定性。

(4) 审计和记录因特网使用量。网络管理员可以在此向管理部门提供因特网连接的费用情况，查出潜在的带宽瓶颈的位置，并能够根据机构的核算模式提供部门级的计费。

(5) 强化网络安全策略。通过以防火墙为中心的安全方案配置，能将所有的安全软件(如口令、加密、身份认证、审计等)配置在防火墙上。与将网络安全问题分散在各个主机上相比，防火墙的集中安全管理更为经济。

6.2.2 防火墙功能局限性

防火墙技术是内部网络最重要的安全技术之一，但防火墙也有其明显的局限性。

(1) 对于绕开了防火墙的攻击行为，防火墙不能提供保护。例如，内部主机可以通过拨号连接互联网业务提供商 ISP 的网络，局域网 LAN 内部可能配置了一个调制解调器池，为出差的雇员和在家中通过网络远程上班的雇员服务。这些都形成了内网与外网的多个接口，从而绕开了防火墙的控制。

（2）防火墙对来自内部的威胁不能提供保护。如一个心怀不满的雇员在网络内部进行攻击。

（3）防火墙不能对那些已经受到病毒感染的程序和文件的传输提供保护。因为在局域网内支持各种操作系统和应用，要求防火墙对所有进入的文件、邮件和信息进行病毒扫描是不现实和不可能的。

6.3　防火墙的分类

防火墙可以按照不同的分类标准进行分类。

6.3.1　以防火墙的软硬件形式分类

1. 软件防火墙

防火墙软件运行于一般的计算机上，需要操作系统的支持，运行防火墙软件的这台计算机承担整个网络的网关和防火墙功能。软件防火墙就像其他软件产品一样，需要先在计算机上安装并做好配置才可以使用。

2. 硬件防火墙

硬件防火墙是由防火墙软件和运行该软件的特定计算机构成。这里的硬件是指这类防火墙包括一个硬件设备，它通常是 PC 架构的计算机。这类防火墙与芯片级防火墙的最大差别在于，它是否是基于专用的硬件平台。目前的大多数硬件防火墙都基于 PC 架构，其本质和普通的 PC 没有太大区别，只不过这些 PC 架构的计算机上运行的是一些经过简化的操作系统。这类防火墙的处理能力比软件防火墙高。

3. 芯片级防火墙

芯片级防火墙基于专门的硬件平台，使用专用的嵌入式实时操作系统。专用的 ASIC 芯片使它们比其他种类的防火墙速度更快，处理能力更强，性能更高。由于使用专用操作系统，防火墙本身的漏洞较少，但价格相对较高。

6.3.2　以防火墙的过滤层次分类

1. 包过滤防火墙

包过滤防火墙工作在 OSI 参考模型的网络层和传输层，可以获取 IP 层和 TCP 层信息，当然也可以获取应用层信息。它根据数据报头的源地址、目的地址、端口号和协议类型等标志确定是否允许通过。只有满足过滤条件的数据报才被转发到相应的目的地，其余数据报则被从数据流中丢弃。包过滤方式是一种简单、有效的安全手段，能够满足绝大多数企业的安全需求。

2. 电路级网关防火墙

电路级网关防火墙用来监控内部网络服务器与不受信任的外部主机间的 TCP 握手信息，以此来决定该会话是否合法。电路级网关是在 OSI 模型的会话层上过滤数据报，其层次比包过滤防火墙高。

3. 应用层网关防火墙

应用层网关防火墙工作在 OSI 的最高层，即应用层。它通过对每一种应用服务编制专

门的代理程序,实现监视和控制应用层通信流的功能。由于应用级网关能够理解应用层协议,所以它能够做一些复杂的访问控制,可执行比较精细的日志和审核,并且能够对数据报进行分析并形成相关的安全报告。不过,因为每一种协议都需要相应的代理软件,所以应用层网关防火墙工作量大,效率不如其他两种防火墙高。

6.3.3 以防火墙应用部署位置分类

1. 边界防火墙

边界防火墙位于内部网络和外部网络的边界,对内部网络和外部网络实施隔离,保护内部网络。这类防火墙一般至少是硬件防火墙类型的,吞吐量大,性能较好。

2. 个人防火墙

安装于单台主机中,仅保护单台主机。这类防火墙应用于个人用户和企业内部的主机,通常为软件防火墙。

3. 混合式防火墙

这是一整套防火墙系统,由若干软、硬件组件组成,分布于内部网络和外部网络的边界、内部网络各主机之间。它既对内部网络和外部网络之间的通信进行过滤,又对网络内部各主机间的通信进行过滤。这类防火墙性能较好,但部署较为复杂。

6.4 防火墙技术

所有防火墙均依赖于对 OSI 参考模型中各层协议所产生的信息流进行检查。任何一个防火墙所能提供的安全保护等级都是与厂商所采用的防火墙技术息息相关的。目前,在各种网络环境中应用的防火墙大多采用了两种基本的技术：包过滤和代理服务。

1. 包过滤技术

包过滤是在网络的适当位置,根据系统设备的过滤规则,对数据报实施过滤,只允许满足过滤规则的数据报通过并将其转发到目的地,而其他不满足规则的数据报则被丢弃。当前大多数的网络路由器都具有一定的包过滤功能。

2. 代理服务技术

代理服务是在防火墙上运行专门的应用程序或服务器程序,这些程序根据安全策略处理用户对网络服务的请求。代理服务位于内部网络和外部网络之间,处理其间的通信以替代相互直接的通信。

6.4.1 过滤型防火墙

1. 静态包过滤防火墙

1）静态包过滤防火墙工作原理

最简单的防火墙形式是静态包过滤防火墙,它一般工作在 TCP/IP 的 IP 层,工作原理如图 6-3 所示。一个静态包过滤防火墙通常是一台有能力过滤数据报部分内容的路由器。当执行包过滤时,包过滤规则被定义在防火墙上,这些规则用来匹配数据报内容以决定哪些包被允许,哪些包被拒绝。当防火墙拒绝通信时,可以采用两个操作,通知通信的发送者其数据将被丢弃,或者没有任何通知直接丢弃这些数据。使用第一个操作时,用户将知道通信

被防火墙过滤掉了，如果这是一个试图访问内部资源的内部用户，该用户可以与管理员联系。如果防火墙不返回一个消息，用户将由于不知道为何不能建立连接而花费更多的时间和精力去解决这个问题。

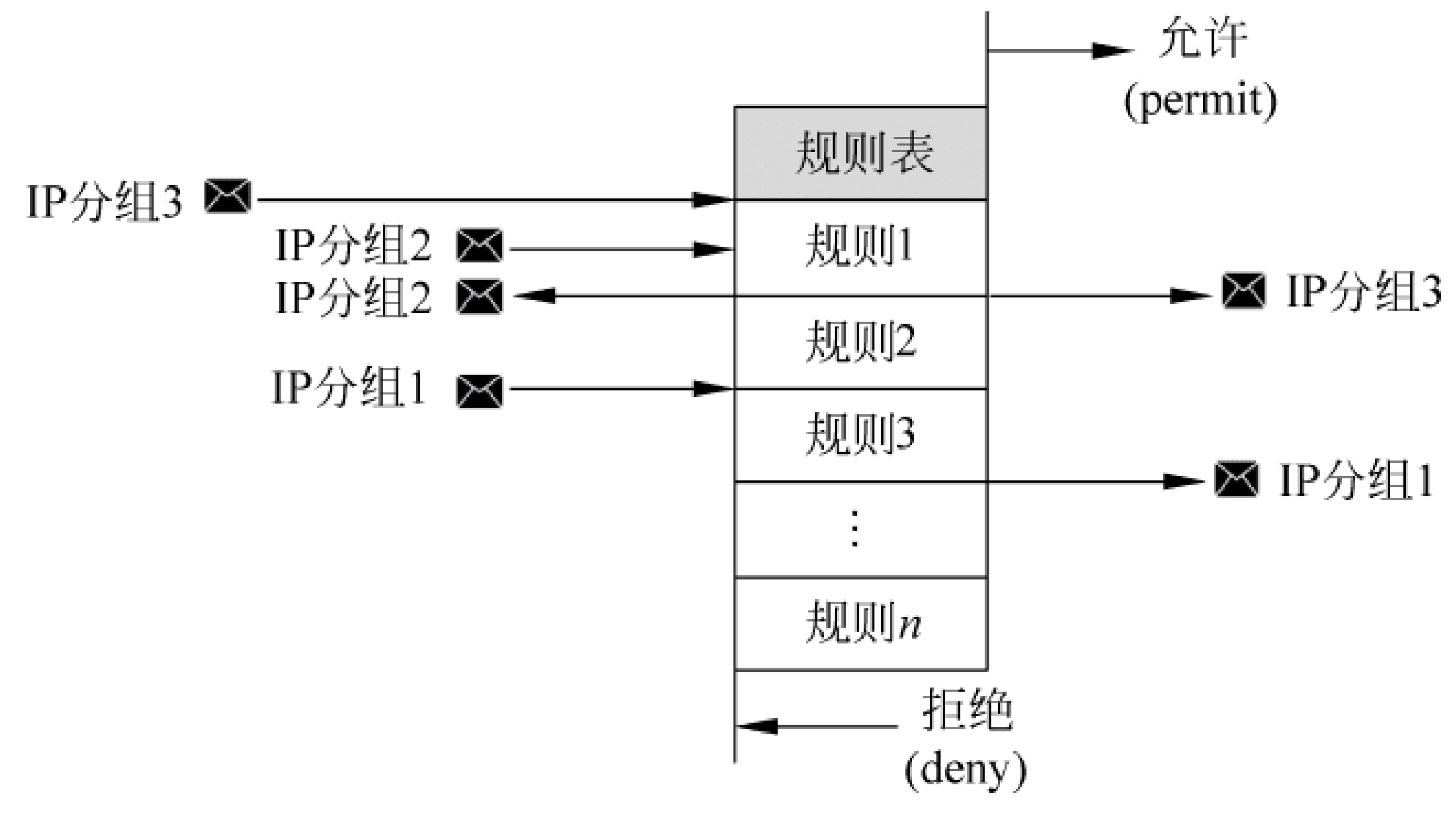


图 6-3　静态包过滤防火墙工作原理示意图

在静态包过滤防火墙上做一个过滤决定时，要用到许多信息。如检查防火墙所使用的过滤表。表 6-1 列出了路由器的包过滤规则。

表 6-1　包过滤规则表

规则	源地址	目的地址	协议类型	端口	操作
1	任意	202.1.1.1	TCP	80	允许
2	任意	202.1.1.2	UDP	53	允许

表 6-1 中，规则 1 说明如果有来自任何设备的数据报被送到 202.1.1.1 的 TCP 端口 80，那么它应该被静态包过滤防火墙允许。同样，规则 2 说明任何数据报被发送到 202.1.1.2 的 UDP 端口 53，那么这些数据报均被允许。除此之外，任何其他类型的数据报都会被丢弃。

2）静态包过滤防火墙优缺点

静态包过滤防火墙的优点是：由于静态包过滤防火墙只是简单根据网络地址、协议和端口进行访问控制，所需进行的处理较少，因此对网络性能的影响比较小，处理速度快，硬件和软件都容易实现；成本较低，配置和使用方法简单，客户端不需要进行特别配置；可以提供附加的网络地址映射功能，可以隐藏内部网络结构。

静态包过滤防火墙的缺点是：不能理解应用层协议，不能对数据分组中更高层的信息进行分析过滤，因而安全性差；不能跟踪连接状态和与应用有关的信息；在支持网络服务的情况下，或者在使用动态分配端口服务的情况下，很难测试用户指定的访问控制规则的有效性；在过滤规则较多、较复杂的情况下，会引起网络性能的下降。

2. 动态包过滤防火墙

1）动态包过滤防火墙工作原理

动态包过滤防火墙又称为状态检测防火墙，它是在静态包过滤防火墙的基础上发展而来的。动态包过滤防火墙的工作原理如图 6-4 所示。在动态包过滤防火墙中有一个状态检测表，它由规则表和连接状态表两部分构成。首先利用规则表进行数据报的过滤，此过程与

静态包过滤防火墙基本相同。如果某个数据报(如“IP 分组 B_1”)在进入防火墙时,规则表拒绝它通过,则防火墙将直接丢弃该数据报,与该数据报相关的后续数据报(如“IP 分组 B_2”“IP 分组 B_3”)同样会被拒绝通过。如果某个数据报(如“IP 分组 A_1”)在进入防火墙时,与该规则表中的某一条规则(如“规则 3”)相匹配,则规则表允许其通过。此时,动态包过滤防火墙会分析已通过的数据报(“IP 分组 A_1”)的相关信息,并在连接状态表中为这次通信过程建立一个连接(如“连接 1”)。之后当同一通信过程中的后续数据报(如“IP 分组 A_2”“IP 分组 A_3”……)进入防火墙时,动态包过滤防火墙不再进行规则表的匹配,而是直接与状态表进行匹配。由于后续的数据报与已经允许通过防火墙的数据报“IP 分组 A_1”具有相同的连接信息,所以会直接允许其通过。

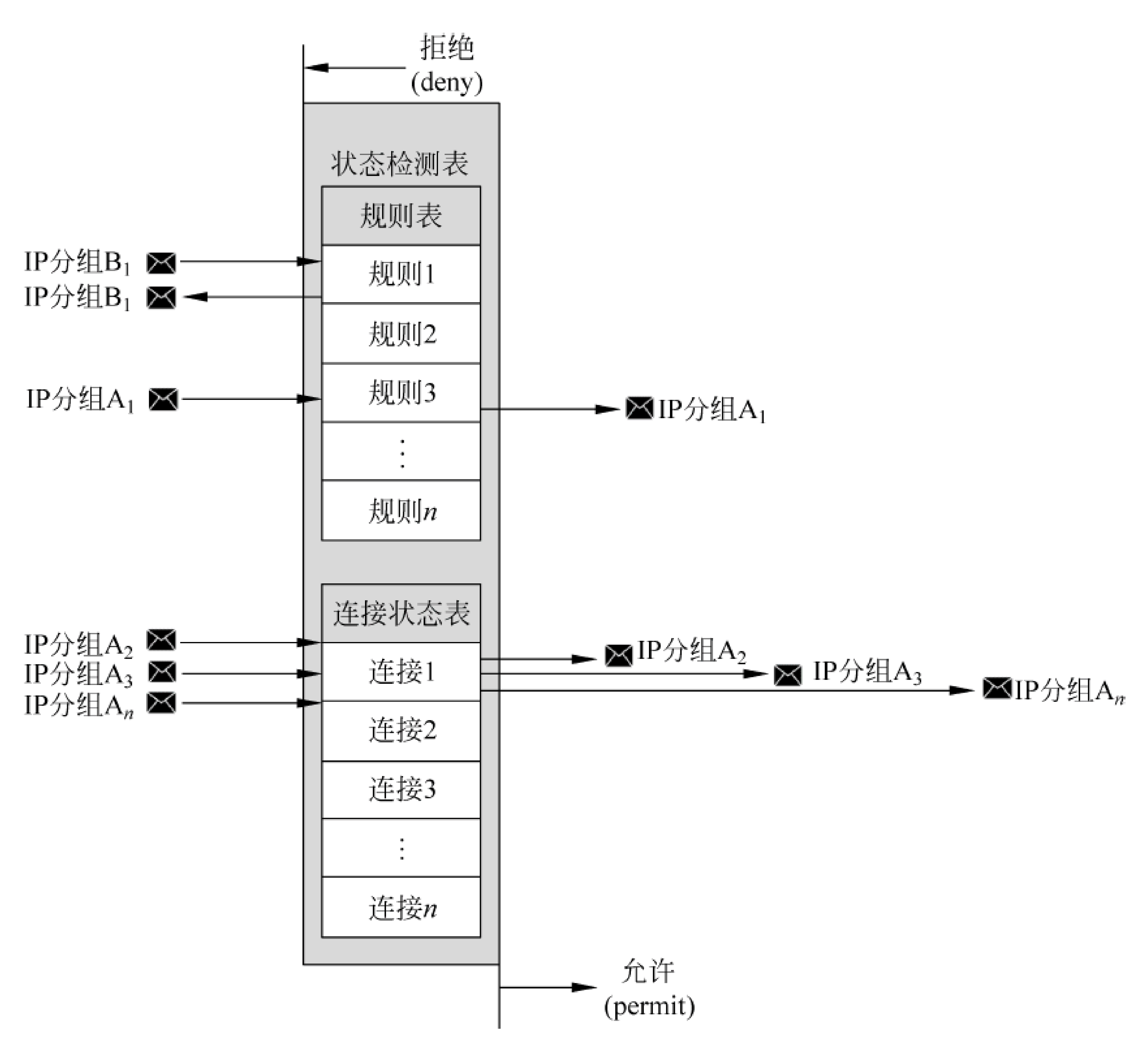


图 6-4　动态包过滤防火墙工作原理示意图

2)动态包过滤防火墙优缺点

动态包过滤防火墙的优点是:与静态包过滤防火墙相比,通过对数据报的跟踪监测技术,解决了静态包过滤防火墙中某些应用在需要使用动态端口时存在的安全隐患,解决了静态包过滤防火墙中存在的一些缺陷;动态包过滤防火墙不需要中断直接参与通信的两台主机之间的连接,对网络速度的影响较小;动态包过滤防火墙具有新型的分布式防火墙的特征,它可以使用分布式探测器对外部网络的攻击进行检测,同时对内部网络的恶意破坏进行防范。

动态包过滤防火墙的缺点是:对防火墙 CPU、内存等硬件要求较高,安全性主要依赖于防火墙操作系统的安全性,安全性不如代理型防火墙。

6.4.2 代理型防火墙

1. 应用级网关防火墙

1）应用级网关防火墙工作原理

应用级网关防火墙通常称为应用代理服务器，它能够检查进出的数据报，通过网关复制传递数据，防止在受信任服务器和客户机与不受信任的主机间直接建立连接，其工作原理如图 6-5 所示。

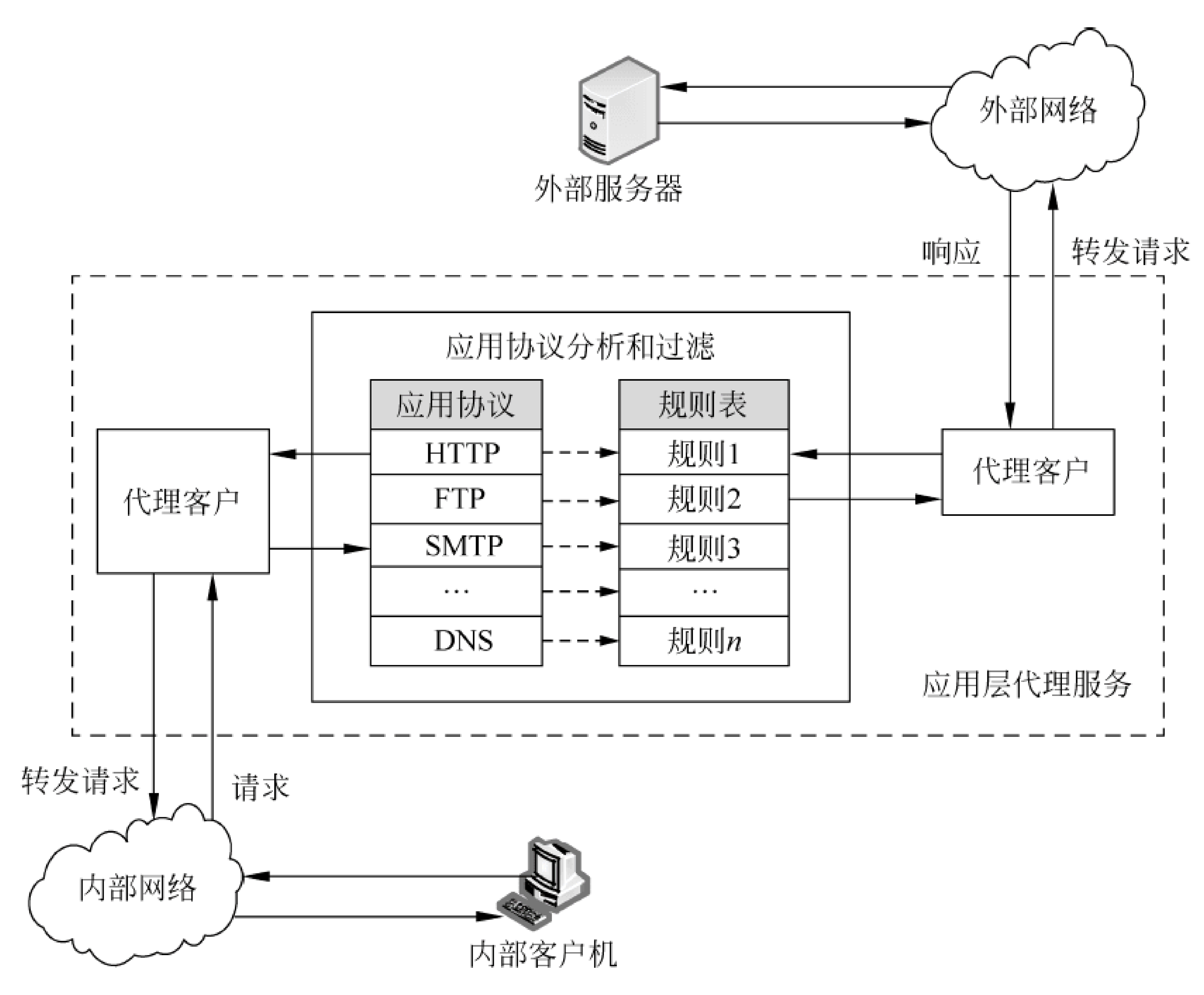


图 6-5 应用级网关防火墙工作原理示意图

应用级网关防火墙必须为特定的应用编写特定的程序，这些程序的集合称为代理服务，它们在网关内部分别以客户机和服务器的形式存在。因此，代理服务是负责处理通过防火墙的某一类特定服务数据流的专用程序。应用级网关防火墙将“客户机/服务器”模型打破，并用两个连接来代替：一个从客户机到防火墙，另一个从防火墙到服务器。

应用级网关防火墙在接受网络连接之前，先在应用层检查网络分组中包含的有效数据，并在连接建立的整个期间检查应用层分组内容，维护详细的连接状态和序列信息。应用级网关防火墙可以验证用户口令和服务请求只在应用层出现的信息。这种机制可以提供增强的访问控制，以实现对有效数据的检查和对传输信息的审计功能，并可以实现一些增值服务（如服务调用审计和用户认证等）。所有调用服务的通信都必须经过网关中的客户机和服务器代理程序过滤。应用级网关防火墙中的代理会接收、传递和过滤由特定服务生成的数据报。如 HTTP 代理只能复制、传递和过滤 HTTP 业务流。又如，如果在应用网关防火墙上运行了 FTP 和 HTTP 代理，只有这两种服务生成的数据能通过防火墙，所有其他的服务均被阻挡。

2）应用级网关防火墙优缺点

应用级网关防火墙的优点是：可以保存关于连接及应用的详细信息，在应用层实现复杂的访问控制；不允许内部网络主机和外部网络服务器之间的直接连接，可隐藏内部地址，安全性高；可以产生丰富的审计记录，便于系统管理员进行分析。

应用级网关防火墙的缺点是：代理服务可能引入不可忽略的处理延时，进入的分组需被处理两次（应用程序和其代理），这样可能会成为网络的瓶颈；对不同的应用服务需要编写不同的代理程序，适应性差，而且无法提供基于UDP或其他协议的代理程序；用户配置较为复杂，增加了系统管理的工作量。

2. 电路级网关防火墙

1）电路级网关防火墙工作原理

电路级网关又称为线路级网关，工作在会话层，是一个通用代理服务器。它适应于多个协议，但不需要识别在同一个协议栈上运行的不同应用，当然也就不需要对不同的应用设置不同的代理模块。它在两个主机首次建立TCP连接时创立一个电子屏障，作为服务器接收外来请求，转发请求；与被保护的主机连接时则担当客户机角色，起代理服务的作用。它监视两主机建立连接时的握手信息，如SYN/ACK和序列数据等是否符合逻辑，判定该会话请求是否合法。一个会话建立后，此会话的信息被写入防火墙维护的有效连接表中。数据报只有在它所含的会话信息符合该有效连接表中的某一入口时，才被允许通过。会话结束时，该会话在表中的入口被删掉。电路级网关只对会话层上的连接进行验证。一旦验证通过，在该连接上可以运行任何一个应用程序，如图6-6所示。

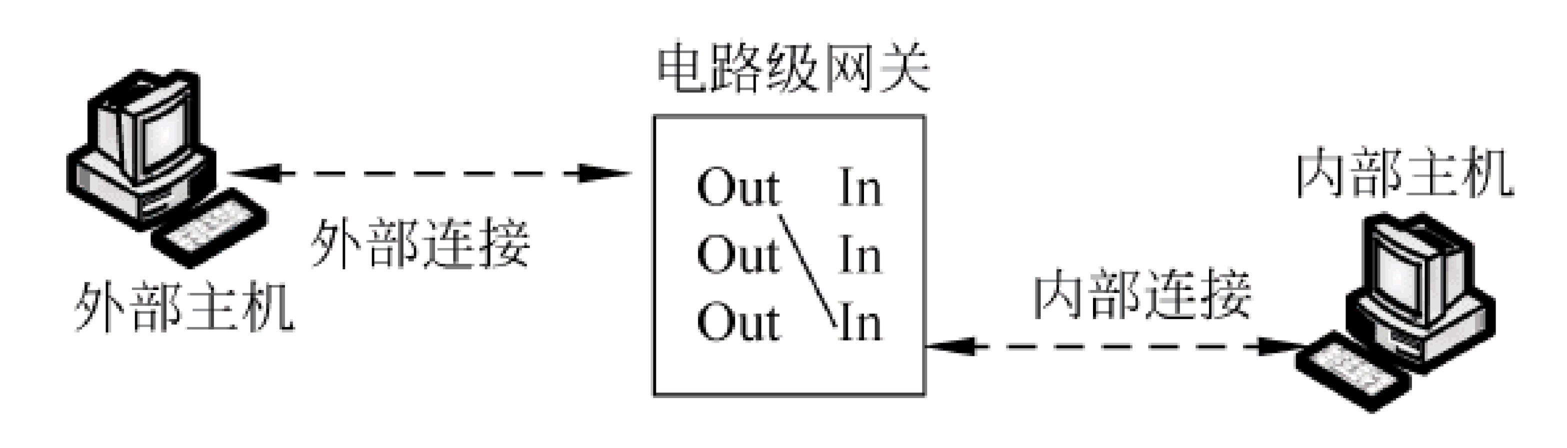


图6-6 电路级网关防火墙工作原理示意图

电路级网关不允许进行端点到端点的TCP连接，而是建立两个TCP连接。一个在网关和内部主机上的TCP用户程序之间，另一个在网关和外部主机的TCP用户程序之间。一旦建立两个连接，网关通常是把TCP数据报从一个连接转送到另一个连接中去而不检验其中的内容，其安全功能就是确定哪些连接是允许的。电路级网关并非作为一个独立的产品存在，它与其他的应用层网关结合在一起。另外，电路级网关还提供一个重要的安全功能——代理服务器。在代理服务器上运行“地址转换”功能，将所有内部的IP地址映射到一个“安全”的IP地址，这个地址是防火墙使用的地址。所以对于外部网络，代理服务器相当于内部网络的一台服务器，而实际上它只是内部网络的一台过滤设备。代理服务器的安全性除了表现在它可以隔断内部和外部网络的直接连接，还表现在它可以防止外部网络发现内部网络的地址。

2）电路级网关防火墙优缺点

电路级网关防火墙的优点是：在OSI上实现的层次较高，可以对更多的元素进行过滤，同时还提供认证功能，安全性比静态包过滤防火墙高；不需要对不同的应用设置不同的代理模块，比应用层网关防火墙具有优势；切断了外部网络到防火墙后面服务器的直接连接，

使数据报不能在服务器与客户机之间直接流动，从而保护了内部网络主机；可以提供网络地址映射功能。

电路级网关防火墙的缺点是：无法进行高层协议的严格安全检查，如无法对数据内容进行检测，以抵御应用层的攻击；对访问限制规则的测试较为困难。

6.5 防火墙体系结构

防火墙的目的在于实现安全访问控制，因此按照 OSI 模型的安全要求，防火墙可以在 OSI 7 层中的 5 层设置。防火墙从功能上分，通常由几个部分组成，如图 6-7 所示。



图 6-7 防火墙组成结构图

目前，防火墙的体系结构一般有以下几种：

(1) 双重宿主主机体系结构；

(2) 屏蔽主机体系结构；

(3) 屏蔽子网体系结构。

6.5.1 双重宿主主机体系结构

双重宿主主机体系结构是围绕具有双重宿主的主机而构建的，该主机至少有两个网络接口。这样的主机可以充当与这些接口相连的网络之间的路由器；它能够从一个网络往另一个网络发送 IP 数据报。然而实现双重宿主主机的防火墙体系结构禁止这种发送功能。因此，IP 数据报并不是从一个网络(如互联网)直接发送到其他网络(如内部的、被保护的网络)。防火墙内部的系统能与双重宿主主机通信，同时防火墙外部的系统也能与双重宿主主机通信，但是这些系统不能直接互相通信，它们之间的 IP 通信被完全阻止。

双重宿主主机的防火墙体系结构是相当简单的，双重宿主主机位于外部系统和内部系统之间，并且被连接到外部网络和内部网络，图 6-8 显示了这种体系结构。

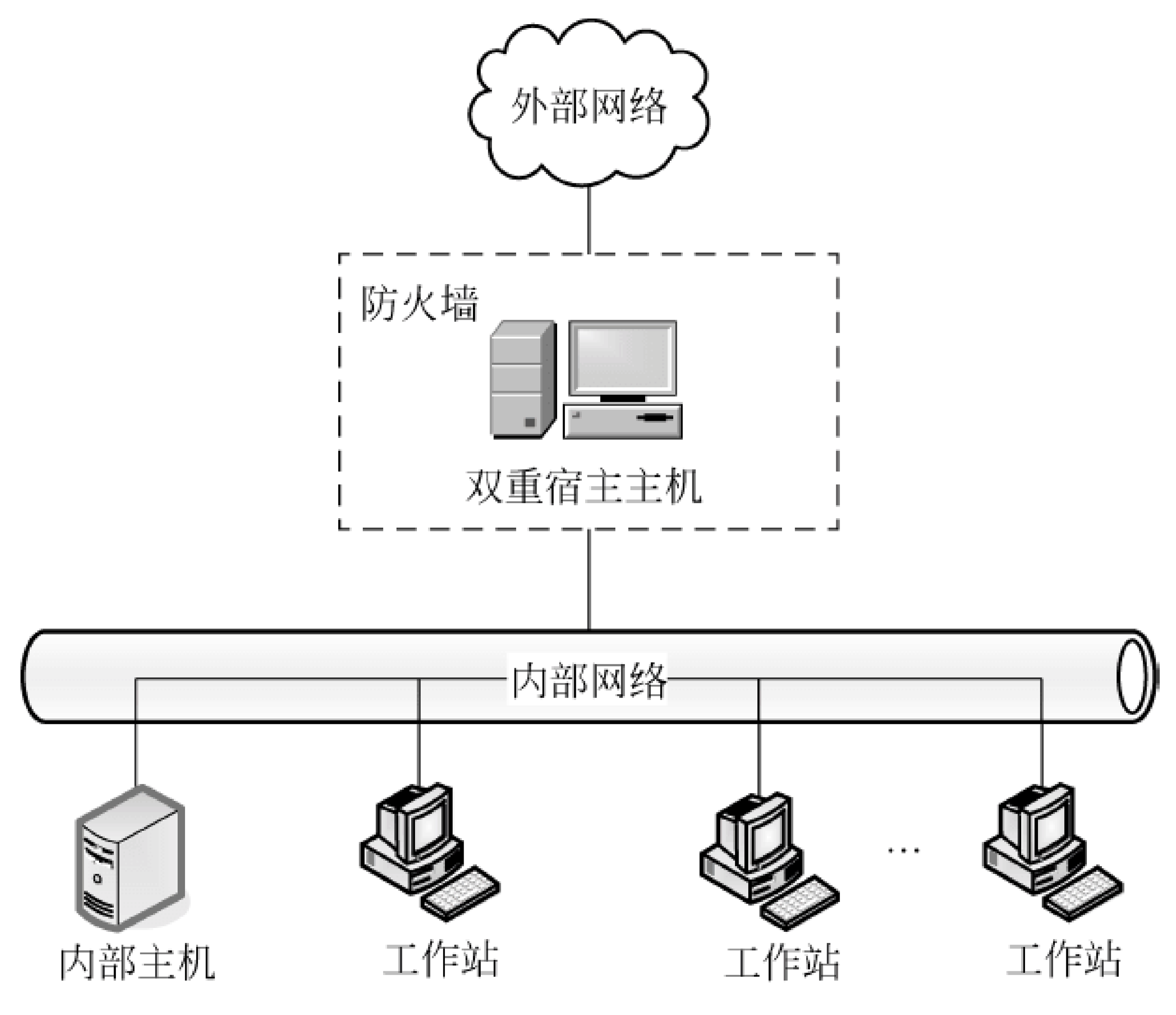


图 6-8 双重宿主主机体系结构

6.5.2 屏蔽主机体系结构

双重宿主主机体系结构是由一台同时连接在内部和外部网络的双重宿主主机提供安全保障的，而屏蔽主机体系结构则不同，在屏蔽主机体系结构中，提供安全保护的主机仅仅与被保护的内部网络相连。屏蔽主机体系结构还使用一个单独的过滤路由器来提供主要安全保护，其结构如图 6-9 所示。

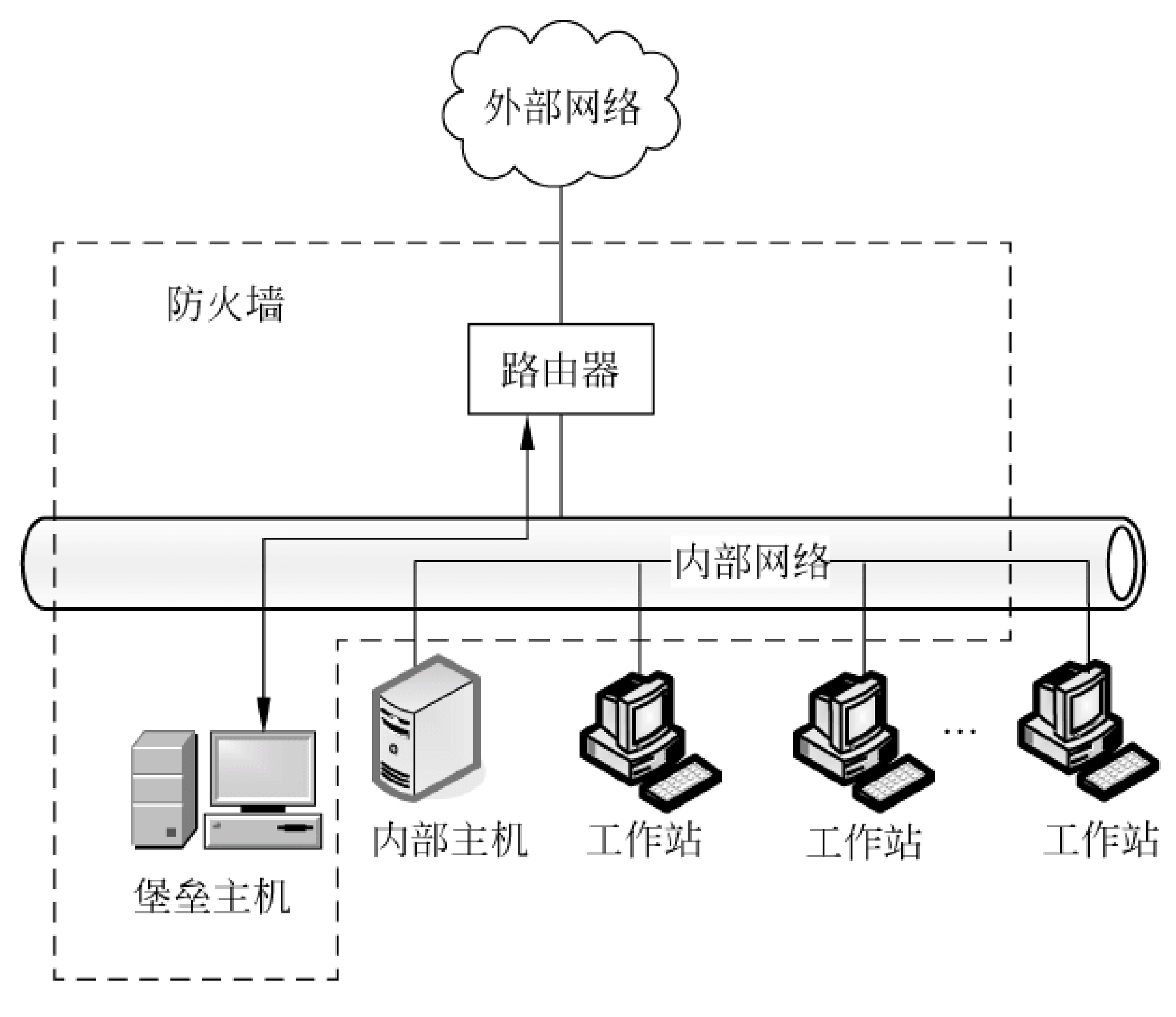


图 6-9　屏蔽主机体系结构

在图 6-9 中，堡垒主机位于内部的网络上，是外部网络上的主机连接到内部网络上的系统的桥梁。即使这样，也仅有某些确定类型的连接被允许，任何外部的系统试图访问内部的系统或者服务将必须连接到这台堡垒主机上。因此堡垒主机需要拥有高等级的安全。数据包过滤也允许堡垒主机开放可允许的连接到外部网络。在该结构的路由器中数据包过滤配置可以按下列方法执行。

(1) 允许其他的内部主机为了某些服务与外部网络上的主机连接(即允许那些已经由数据包过滤的服务)。

(2) 不允许来自内部主机的所有连接。用户可以针对不同的服务混合使用这些手段：某些服务可以被允许直接经由数据包过滤，而其他服务仅仅可以被允许间接地经过代理。这完全取决于用户实行的安全策略。

因为这种体系结构允许数据包从外部网向内部网移动，所以，它的设计比没有外部数据包能到达内部网络的双重宿主主机体系结构似乎更冒风险。但实际上，双重宿主主机体系结构在防备数据包从外部网络穿过内部网络时，也容易失败(如黑客入侵)。另外，保护路由器比保护主机更易实现，因为它提供非常有限的服务组。在多数情况下，被屏蔽的主机体系结构能提供比双重宿主主机体系结构更强的安全性和可用性。

6.5.3 屏蔽子网体系结构

屏蔽子网体系结构添加额外的安全层到屏蔽主机体系结构，即通过添加周边网络更进一步地把内部网络与因特网隔离开。

堡垒主机是用户网络上最容易被攻击的计算机。虽然用户尽最大的力气去保护它，它仍是最有可能被入侵的计算机。在屏蔽主机体系结构中，堡垒主机一旦被攻破，被保护的内部网络就会在外部入侵者面前门户洞开，因为在堡垒主机与内部网络的其他内部计算机之间没有其他的防御手段。如果有人成功地入侵屏蔽主机体系结构中的堡垒主机，那就等于进入了内部系统。

通过用周边网络隔离堡垒主机，能减少堡垒主机被入侵造成的影响。即它只给入侵者一些访问的机会，而不是全部机会。屏蔽子网体系结构的最简单的形式为两个屏蔽路由器，每一个都连接到周边网。一个位于周边网与保护的内部网络之间，另一个位于周边网与外部网络之间，其结构如图 6-10 所示。

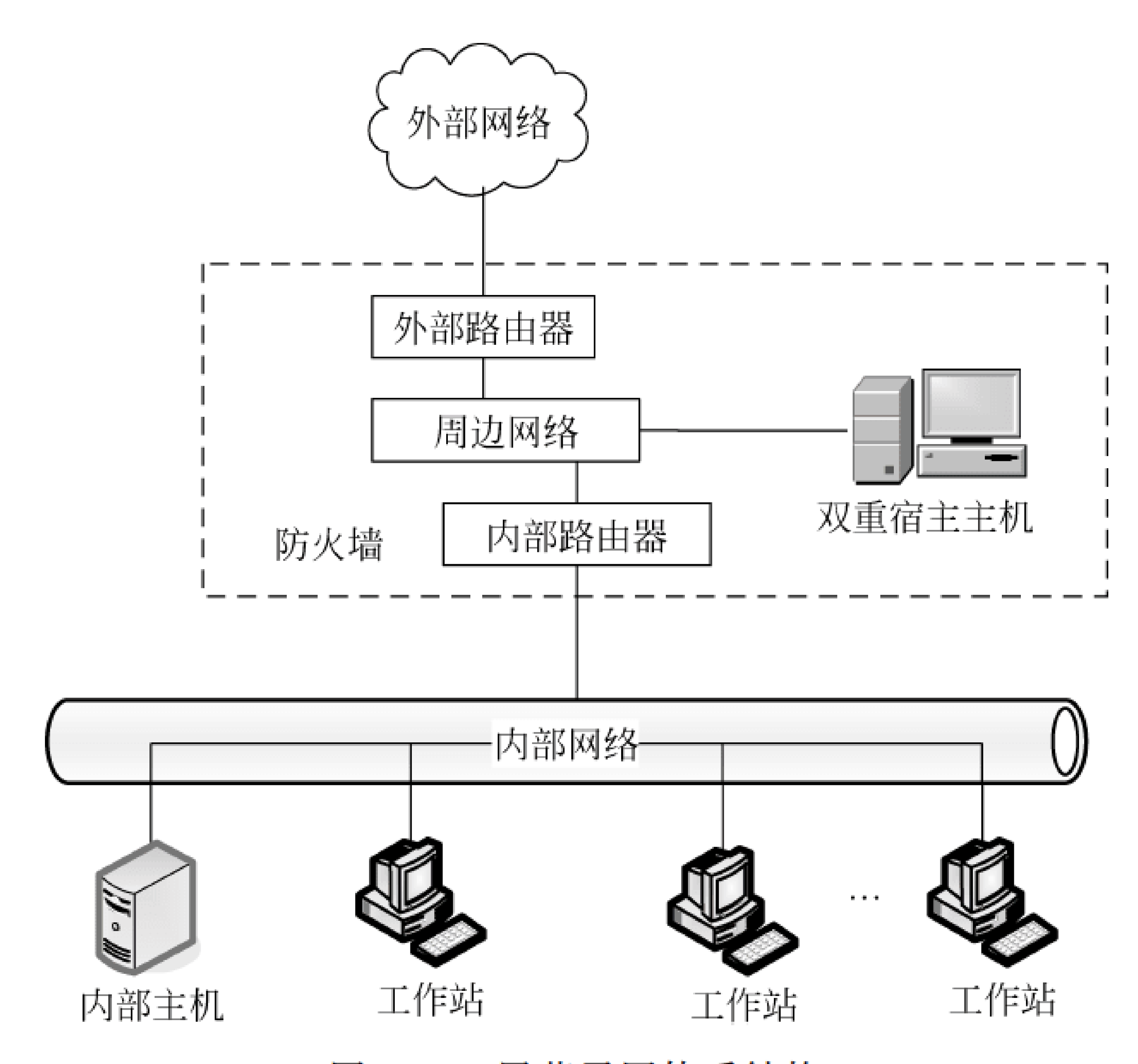


图 6-10　屏蔽子网体系结构

为了入侵用屏蔽子网体系结构保护的内部网络，入侵者必须通过两个路由器。即使入侵者设法侵入了堡垒主机，他仍然必须通过内部路由器。

下面介绍在这种结构里所采用的组件。

1. 周边网络

周边网络是另一个安全层，是在外部网络与被保护的内部网络之间附加的网络。如果入侵者成功地入侵用户的防火墙的外层领域，周边网络在那个入侵者与用户的内部系统之间提供一个附加的保护层。

2. 堡垒主机

在屏蔽子网体系结构中，用户把堡垒主机连接到周边网络，这台主机便是接受来自外界连接的主要入口。它为内部网络提供的服务如下。

(1) 接收外来的电子邮件，再分发给相应的站点。

(2) 接收外来的 FTP 连接，再转接到内部网络的匿名 FTP 服务器。

(3) 接收外来的对有关内部网络站点的域名服务查询。

另一方面，这台堡垒主机向外部网络提供的服务通过以下方法实施。

（1）在外部和内部的路由器上设置数据包过滤来允许内部的客户端直接访问外部的服务器。

（2）设置代理服务器在堡垒主机上运行，允许内部网络的用户间接地访问外部网络的服务器。也可以设置数据包过滤，允许内部网络的用户与堡垒主机上的代理服务器进行交互，但是禁止内部网络的用户直接与外部网络进行通信。

3. 内部路由器

内部路由器（阻塞路由器）保护内部的网络使之免受外部网络和周边网络的侵犯。内部路由器完成防火墙的大部分数据包过滤工作。它允许从内部网络到外部网络的有选择的外连服务。这些服务是根据内部网络的需要和安全规则选定的，如 telnet、FTP 等。内部路由器可以设定，使周边网络上的堡垒主机与内部网络之间传递的各种服务不同于内部网络和外部网络之间传递的各种服务。限制堡垒主机和内部网络之间服务的理由是减少由此而导致的受到来自堡垒主机侵袭的机器数量。

4. 外部路由器

在理论上，外部路由器（访问路由器）保护周边网络和内部网络，使之免受来自外部网络的入侵。实际上，外部路由器倾向于几乎让所有周边网络的外出请求通过，通常只执行非常少的数据包过滤。保护内部计算机的数据包过滤规则在内部路由器和外部路由器上基本一致，如果在规则中有允许入侵者访问的错误，错误就可能出现在两个路由器上。

由于外部路由器一般由外界提供，如用户的互联网服务提供商 ISP，所以用户对外部路由器的访问是受限制的。ISP 可能愿意放入一些通用型数据包过滤规则来维护路由器，但是不愿意使用维护复杂或者频繁变化的过滤规则。因此对于安全保障而言，不能像依靠内部路由器那样依靠外部路由器。

外部路由器能有效地执行的安全任务是：阻断从外部网络上伪造源地址进来的任何数据包。这样的数据包自称来自内部网络，但实际上是来自外部网络。

6.6 防火墙选择原则

当我们在规划网络时，不能不考虑整体网络的安全性。而谈到网络安全，就不能忽略防火墙的功能，防火墙产品有上千种，如何在其中选择最符合需要的产品，是消费者最关心的事。一个好的防火墙必须具备以下特点。

1. 是一个整体网络的保护者

好的防火墙应该以整体网络保护者自居，它所保护的对象应该是全网而不仅是那些通过防火墙的使用者。

2. 能弥补其他操作系统的不足

好的防火墙必须是建立在操作系统之间而不是在操作系统之后，所以操作系统有些漏洞并不会影响到其所提供的安全性。由于硬件平台的普及以及执行效率的因素，大部分企业经常把对外提供各种服务的服务器分散在许多操作系统平台上，我们在无法保证所有主机安全的情况下，选择防火墙作为整体安全的保护者。这正说明了操作系统提供 B 级或是 C 级的安全并不一定会直接对整体安全造成影响，是因为一个好的防火墙必须能弥补操作系统的不足。

3. 为使用者提供不同平台的选择

由于防火墙并非完全由硬件构成，因此软件(操作系统)所提供的功能以及执行效率一定会影响到整体的表现，而使用者的操作意愿及对防火墙软件的熟悉程度也是必须考虑的重点。一个好的防火墙不但本身要有良好的执行效率，也应该提供多平台的执行方式供使用者选择，毕竟使用者才是安全的控制者。使用者应该选择一套符合当前环境需求的软件，而不应为了软件的限制而改变现有环境。

4. 能向使用者提供完善的售后服务

由于有新产品的出现，就会有人研究新的破解方法，因此一个好的防火墙提供者必须有一个庞大的组织作为使用者的安全后盾，也应该有众多的使用者所建立的口碑为防火墙做见证。防火墙安装和投入使用后，并非万事大吉，要想充分发挥它的安全防护作用，必须对它进行跟踪和维护，这就需要与商家保持密切的联系，时刻关注商家的动态。因为商家一旦发现其产品存在安全漏洞，就会尽快发布补救产品，此时用户应尽快确认其真伪(防止特洛伊木马等病毒)，并对防火墙软件进行更新。

5. 提供完整的安全检查功能

好的防火墙应该向使用者提供完整的安全检查功能，但是一个安全的网络仍必须依靠使用者的观察及改进。

6. 能实现 IP 转换

IP 转换能隐藏内部网络真正的 IP，使入侵者无法直接入侵内部网络，另外节省的 IP 作为内部使用。

7. 有双重 DNS

当内部网络使用没有注册的 IP 地址或是防火墙进行 IP 转换时，DNS 也必须经过转换，同样一个主机在内部的 IP 与给予外界的 IP 将会不同，所以双重 DNS 防火墙是很必要的。

8. 具有查杀的功能

大部分防火墙都可以与防病毒防火墙搭配，实现查杀病毒功能，有的防火墙甚至可以直接集成扫毒功能和杀毒功能。

6.7 某企业销售系统中防火墙建立实例

1. 企业需求分析

假设某企业设有人事部、生产部、计划部、市场部、采购部。

2. 防火墙系统设计方案

1) 方案一

如图 6-11 所示，该系统由于 Web 服务器在防火墙之外，可以满足企业建立主页以宣传企业形象、企业内部信息交流和保护内部网络安全等基本要求，因此对于内部数据安全要求不高的小型企业，此方案是适合的。

但是，一旦黑客攻破了防火墙，整个内部网络就处在完全暴露的状态。而且，在外地的销售人员或市场分部与本部的联系易造成安全漏洞，内部的敏感数据只有依靠口令、加密和授权来管理保护。

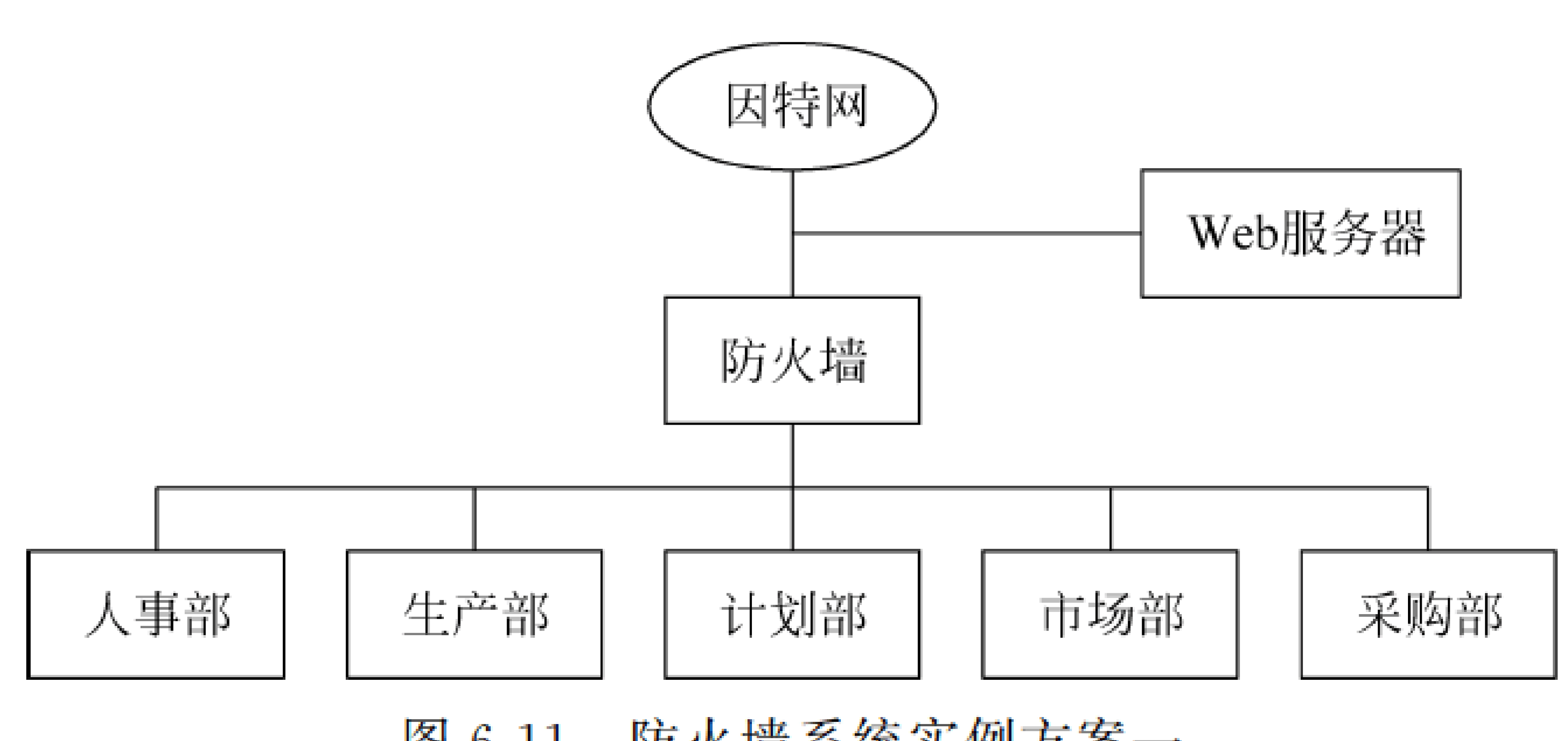


图 6-11　防火墙系统实例方案一

2）方案二

如图 6-12 所示，Web 服务器放在防火墙之内，有利于企业对 Web 服务器上的企业主页进行管理和维护。而且，外部用户访问它时必须通过防火墙，可防止大量的非法入侵，外部用户访问内部网络时，还需再经过访问服务器的过滤，进一步加强了安全性。同时内部用户访问因特网受到限制，如只允许 E-mail 通过。

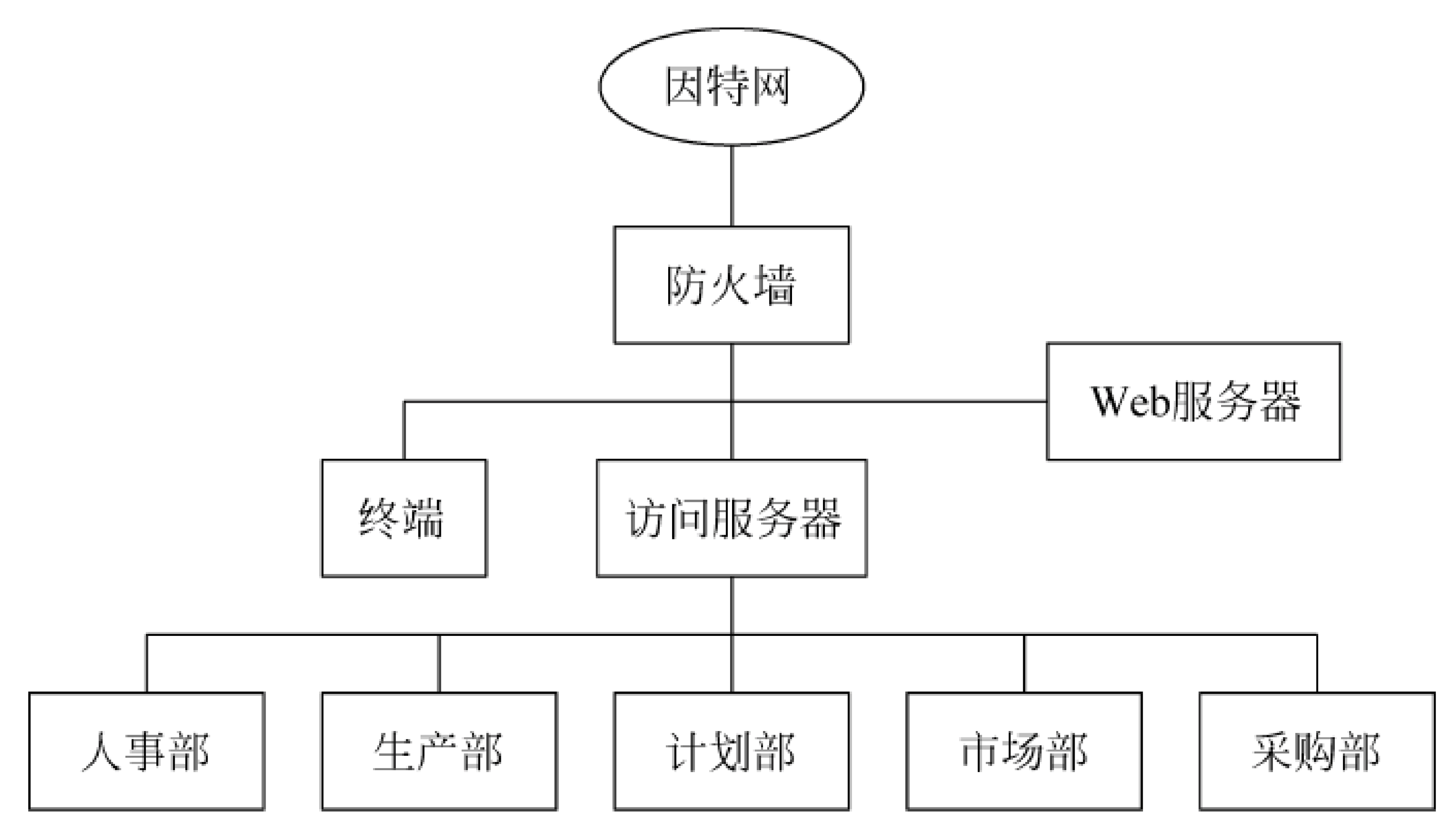


图 6-12　防火墙系统实例方案二

3）方案三

如图 6-13 所示，在前面的两个方案中，都没有考虑企业内部数据的保护问题。实际上，各个部门之间有些数据是相互公开的，而有些数据只能提供本部门或部门内的少数人使用，例如采购部的数据。所以，为了防止来自内部的攻击，需要对内部网络使用防火墙隔离，这样就可以构建比较完整的防火墙安全系统。

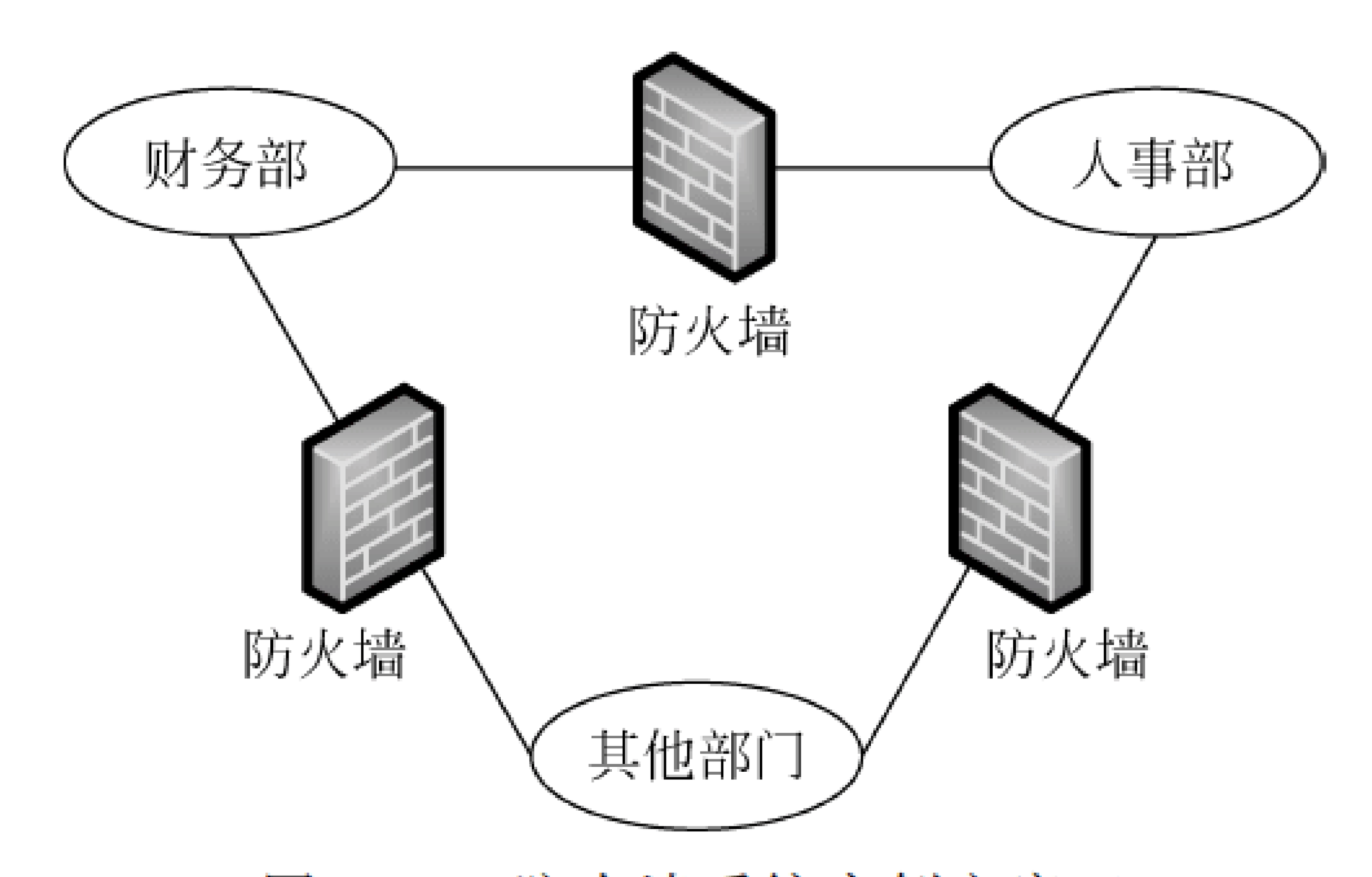


图 6-13　防火墙系统实例方案三

6.8 防火墙配置

6.8.1 PIX 防火墙配置

PIX 是 Cisco 的硬件防火墙，硬件防火墙有工作速度快、使用方便等特点。配置 PIX 防火墙有 6 个基本命令：nameif、interface、ip address、nat、global、route。这些命令在配置 PIX 是必需的。

1. 配置防火墙接口的名字，并指定安全级别(nameif)

```
Pix525(config)#nameif ethernet0 outside security0
Pix525(config)#nameif ethernet1 inside security100
```

说明：在默认配置中，以太网 0 被命名为外部接口(outside)，安全级别是 0；以太网 1 被命名为内部接口(inside)，安全级别是 100。安全级别取值范围为 1～100，数字越大安全级别越高。若设置 ethernet2 为中间接口 dmz，安全级别为 50，配置命令如下：

```
Pix525(config)#nameif ethernet2 dmz security50
```

2. 配置以太口参数(interface)

```
Pix525(config)#interface ethernet0 auto
Pix525(config)#interface ethernet1 100full
Pix525(config)#interface ethernet1 100full shutdown
```

说明：auto 选项表明系统自适应网卡类型。100full 选项表示 100Mb/s 以太网全双工通信。shutdown 选项表示关闭这个接口，若启用接口去掉 shutdown。

3. 配置内外网卡的 IP 地址(ip address)

```
Pix525(config)#ip address outside 64.124.50.13 255.255.255.248
Pix525(config)#ip address inside 192.168.1.1 255.255.255.0
```

说明：Pix525 防火墙在外网的 IP 地址是 64.124.50.13，内网 IP 地址是 192.168.1.1。

4. 指定要进行转换的内部地址(nat)

网络地址转换(nat)作用是将内网的私有 IP 转换为外网的公有 IP。nat 命令总是与 global 命令一起使用，这是因为 nat 命令可以指定一台主机或一段范围的主机访问外网，访问外网时需要利用 global 所指定的地址池进行对外访问。nat 命令配置语法格式如下：

```
nat (if_name) nat_id local_ip [netmark]
```

其中(if_name)表示内网接口名字，例如 inside。nat_id 用来标识全局地址池，使它与其相应的 global 命令相匹配，local_ip 表示内网被分配的 IP 地址。例如 0.0.0.0 表示内网所有主机可以对外访问。[netmark]表示内网 IP 地址的子网掩码。

例 1：Pix525(config)#nat (inside) 1 0 0

说明：表示启用 nat，内网的所有主机都可以访问外网，用 0 可以代表 0.0.0.0

例 2：Pix525(config)#nat (inside) 1 172.16.5.0 255.255.0.0

说明：表示只有 172.16.5.0 这个网段内的主机可以访问外网。

5. 指定外部地址范围(global)

global 命令把内网的 IP 地址翻译成外网的 IP 地址或一段地址范围。global 命令的配置语法格式如下：

```
global (if_name) nat_id ip_address - ip_address [netmark global_mask]
```

其中(if_name)表示外网接口名字,例如 outside。nat_id 用来标识全局地址池,使它与其相应的 nat 命令相匹配,ip_address-ip_address 表示翻译后的单个 IP 地址或一段 IP 地址范围。[netmark global_mask]表示全局 IP 地址的网络掩码。

例 3：Pix525(config)# global (outside) 1 64.124.50.13-64.124.50.18

说明：表示内网的主机通过 PIX 防火墙要访问外网时,PIX 防火墙将使用 64.124.50.13～64.124.50.18 这段 IP 地址池为要访问外网的主机分配一个全局 IP 地址。

例 4：Pix525(config)# global (outside) 1 64.124.50.13

说明：表示内网要访问外网时,PIX 防火墙将为访问外网的所有主机统一使用 64.124.50.13 这个单一 IP 地址。

例 5：Pix525(config)# no global (outside) 1 64.124.50.13

说明：表示删除这个全局表项。

6. 设置指向内网和外网的静态路由(route)

定义一条静态路由。route 命令配置语法格式如下：

```
route (if_name) 0 0 gateway_ip [metric]
```

其中(if_name)表示接口名字,例如 inside 和 outside。gateway_ip 表示网关路由器的 IP 地址。[metric]表示到 gateway_ip 的跳数。通常默认是 1。

例 6：Pix525(config)# route outside 0 0 61.144.51.168 1

说明：表示一条指向边界路由器(IP 地址 61.144.51.168)的默认路由。

例 7：Pix525(config)# route inside 10.1.1.0 255.255.255.0 172.16.1.1 1

说明：如果内部网络只有一个网段,按照例 1 那样设置一条默认路由即可；如果内部存在多个网络,需要配置一条以上的静态路由。上面那条命令表示创建了一条到网络 10.1.1.0 的静态路由,静态路由的下一条路由器 IP 地址是 172.16.1.1

6.8.2 VRP3 防火墙配置

通用路由平台(Versatile Router Platform,VRP)是华为公司数据通信产品的通用网络操作系统平台,它实现了 OSPF、BGP、RIP、EIGRP 等多种单播和多播路由协议,支持路由迭代、路由策略和路由聚合等丰富的路由特性,VRP 中的防火墙主要是指基于访问控制列表(ACL)的包过滤、基于应用层的包过滤防火墙 ASPF 和地址转换。

1. ACL 包过滤防火墙配置

ACL 包过滤应用在路由器中,为路由器增加了对数据包的过滤功能。ACL 包过滤实现对 IP 数据报的过滤,对路由器需要转发的数据包,先获取数据包的包头信息,包括 IP 层所承载的上层协议的协议号,数据包的源地址、目的地址、源端口和目的端口等,然后和设定 ACL 规则进行比较,根据比较的结果决定对数据包进行转发或者丢弃。ACL 包过滤提供了对分片报文检测过滤的支持。包过滤防火墙将检测报文类型分为非分片报文、首片分片

报文和非首片分片报文。获得报文的三层(IP 层)信息(基本 ACL 规则和不含三层以外信息的高级 ACL 规则)及三层以外的信息(包含三层以外信息的高级 ACL 规则)用于匹配,并获得配置的 ACL 规则。对于配置了精确匹配过滤方式的高级 ACL 规则,包过滤防火墙需要记录每一个首片分片的三层以外的信息,当后续分片到达时,使用这些保存的信息对 ACL 规则的每一个匹配条件进行精确匹配。应用精确匹配过滤后,包过滤防火墙的执行效率会略微降低,配置的匹配项目越多,效率降低越多,可以配置门限值为限制防火墙最大处理的数目。

ACL 包过滤防火墙主要需要配置步骤如下。

(1) 允许或禁止防火墙。在系统视图输入操作命令:

```
firewall enable
```

如果是禁止防火墙,输入 undo firewall enable。系统默认情况下禁止防火墙。

(2) 设置防火墙默认过滤方式。在系统视图输入操作命令:

```
firewall default permit
```

如果设置默认过滤方式为禁止通过,输入 firewall default deny。在防火墙开启时,系统默认允许。

(3) 设置包过滤防火墙分片报文检测开关。在系统视图中输入操作命令:

```
firewall fragments - inspect
```

如果需要关闭分片报文检测开关,输入 undo firewall fragments-inspect。注意,只有打开了分片报文检测开关,精确匹配模式才能真正有效。

(4) 配置分片报文检测的上、下门限值,在系统视图输入操作命令:

```
firewall fragments - inspect{high | low}{default | number}
```

如果恢复上限分片状态记录数目为默认值,输入 undo firewall fragments-inspect{high | low}。注意:默认的上限分片状态记录数目为 2000,下限分片状态记录数目为 1500。

(5) 在接口上应用访问控制列表,在接口视图输入操作命令:

```
firewall packet - filter { acl - number | acl - name}{inbound | outbound}[match - fragments
{normally | exactly}]
```

如果取消接口上过滤接收报文的规则,输入 undo firewall packet-filter{acl-number | acl-name}{inbound | outbound}。

(6) 包过滤防火墙显示与调试。

在完成上述配置后,在所有视图下执行如下 display 命令可以显示包过滤防火墙的运行情况,通过查看显示信息验证配置的效果。执行如下 debugging 命令可以对包过滤防火墙进行调试。

```
display firewall - statistics {all | interface interface - name | fragments - inspect}
#显示接口的有关防火墙的统计信息
debugging firewall { all | icmp | tcp | udp | others}[interface interface - name]
#打开防火墙包过滤调试信息开关
```

```
undo debugging firewall { all | icmp| tcp | udp | others}[interface interface - name]
#关闭防火墙包过滤调试信息开关
```

2. 防火墙配置实例

下面通过一个公司配置防火墙的实例来说明防火墙的配置。

该公司通过一台 Quidway 路由器的接口 Serial1/0/0 访问因特网，路由器与内部网通过以太网接口 Ethernet0/0/0 连接。公司内部对外提供 WWW、FTP 和 telnet 服务，公司内部子网为 126.45.8.0，其中，内部 FTP 服务器地址为 126.45.8.1，内部 telnet 服务器地址为 126.45.8.2，内部 WWW 服务器地址为 126.45.8.3，公司对外地址为 202.32.1.1。在路由器配置了地址转换，这样内部主机可以访问因特网，外部主机可以访问内部服务器。通过配置防火墙，希望实现以下要求：

(1) 外部网络只有特定用户可以访问内部服务器。

(2) 内部网络只有特定主机可以访问外部网络。

(3) 假定外部特定用户的 IP 地址为 202.33.3.2。

具体的配置步骤如下所示。

```
#在路由器 Quidway 上允许防火墙
[Quidway] firewall enable
#设置防火墙默认过滤方式为允许包通过
[Quidway] firewall default permit
#创建访问控制列表 101
[Quidway] acl number 101
#配置规则禁止所有 IP 包通过
[Quidway - acl - adv - 101] rule deny ip
#配置规则允许特定主机访问外部网,允许内部服务器访问外部网
[Quidway - acl - adv - 101] rule permit ip source 126.45.8.1 0
[Quidway - acl - adv - 101] rule permit ip source 126.45.8.2 0
[Quidway - acl - adv - 101] rule permit ip source 126.45.8.3 0
#创建访问控制列表
[Quidway] acl number 102
#配置规则允许特定用户从外部网访问内部服务器
[Quidway - acl - adv - 102] rule permit tcp source 202.33.3.2 0 destination 202.32.1.1 0
#配置规则允许特定用户从外部网取得数据(只允许端口大于 1024 包)
[Quidway - acl - adv - 102] rule permit tcp destination 202.32.1.10 0 destination - port gt 1024
#将规则 101 作用于从接口 Ethernet0/0/0 进入的包
[Quidway - Ethernet0/0/0] firewall packet - filter 101 inbound
#将规则 102 作用于从接口 Serial1/0/0 进入的包
[Quidway - Serial1/0/0] firewall packet - filter 102 inbound
```

3. ASPF 配置

ASPF(Application Specific Packet Filter)是针对应用层的包过滤，即基于状态的报文过滤。它和普通的静态防火墙协同工作，以便于实施内部网络的安全策略。ASPF 能够检测试图通过防火墙的应用层协议会话信息，阻止不符合规则的数据报文通过。为保护网络安全，基于访问控制列表的包过滤可以在网络层和传输层检测数据包，防止非法入侵。ASPF 能够检测应用层协议的信息，并对应用的流量进行监控，同时能针对 DoS 进行检测和防范，使用 Java Blocking(Java 阻断)来保护网络不受有害的 Java Appets 的破坏。它还支

持端口到应用的映射，用于应用层协议提供的服务使用非通用端口时的情况。它增强了会话日志功能，可以对所有的连接进行记录，包括记录连接的时间、源地址、目的地址、使用的端口和传输的字节数。ASPF 对应用层的协议信息进行检测，并维护会话的状态，检查会话的报文的协议和端口号等信息，阻止恶意的入侵。ASPF 能对如下协议的流量进行监测：FTP、HTTP、SMTP、RSTP、H.323、TCP 和 UDP。

ASPF 配置中需要允许防火墙使用，同时配置访问控制列表，然后定义一个 ASPF 策略，最后在选定的接口上应用。

下面介绍如何定义一个 ASPF 策略。

（1）创建一个 ASPF 策略，在系统视图下操作命令：

```
aspf - policy aspf - policy - number
```

如果删除创建一个 ASPF 策略，输入 undo aspf-policy aspf-policy-number，其中 aspf-policy-number 为 ASPF 策略号，范围为 1～99。

（2）配置空闲超时值，在系统视图下操作命令：

```
aging - time{syn | fin | tcp | udp}seconds
```

如果恢复默认的空闲超时值，输入 undo aging-time{syn | fin | tcp | udp}。

该任务用来配置 TCP 的 SYN 状态等待超时值、FIM 状态等待超时值，TCP 和 UDP 会话表项空闲状态超时值。默认情况下 syn、fin、tcp、udp 的超时时间分别为 30s、5s、3600s 和 30s。

（3）配置应用层协议检测，在系统视图下操作命令：

```
detect protocol [aging - time seconds]
```

如果要删除配置的应用协议检测，输入 undo detect protocol。

应用层协议 protocol 可取值 ftp、smtp、http。在 protocol 选择 http 时，可以配置 Java 阻断，在系统视图下操作命令：

```
detect http{java - list acl - number}[aging - time seconds]
```

如果取消对 HTTP 的检测规则，输入 undo detect http。

（4）配置一般 TCP 和 UDP 检测，在 ASPF 策略视图下操作命令：

```
#配置通用 TCP 协议检测
detect tcp [aging - time seconds]
#配置通用 UDP 协议检测
detect udp[aging - time seconds]
#删除通用 TCP 协议检测
undo detect tcp
#删除通用 UDP 协议检测
undo detect udp
```

（5）在接口上应用，在接口视图下，输入如下命令：

```
firewall aspf aspf - policy - number{inbound | outbound}
```

如果删除该接口上应用的 ASPF 策略，输入 undo firewall aspf aspf - policy - number{inbound | outbound}

(6) ASPF 显示与调试。

在完成上述配置后，在所有视图下执行如下 display 命令可以显示 ASPF 的运行情况，通过查看显示信息验证配置的效果。在用户视图下执行 debugging 命令查看 ASPF 调试信息。

```
#显示所有 ASPF 配置情况
display aspf all
#显示应用 ASPF 策略和访问列表的接口配置
display aspf interface
#显示一个特定 ASPF 策略的配置
display aspf policy aspf-policy-number
#显示 ASPF 当前会话状态
display aspf session
#打开 ASPF 调试开关
debugging aspf{all | detail | events | ftp | http | rtsp | session | smtp | tcp | timer | udp}
#关闭 ASPF 调试开关
undo debugging aspf{all | detail | events | ftp | http | rtsp | session | smtp | tcp | timer | udp}
```

4. ASPF 策略配置实例

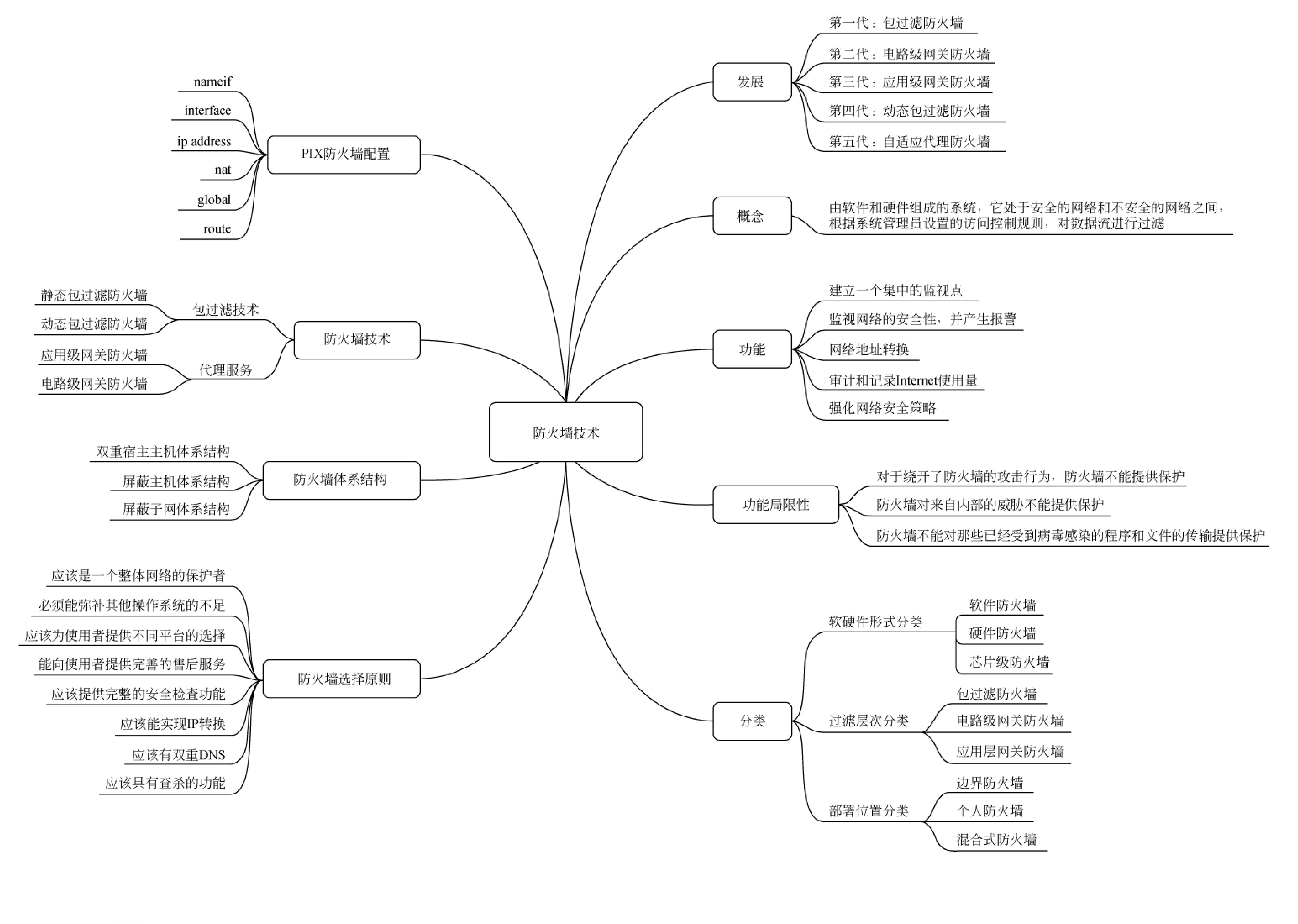
下面在防火墙上具体配置一个 ASPF 策略，来检测通过防火墙的 FTP 和 HTTP 流量。如果该报文是内部网络用户发起的 FTP 和 HTTP 连接的返回报文，则允许其通过防火墙进入内部网络，其他报文被禁止；并且，此 ASPF 策略能够过滤掉来自服务器 122.35.2.1 的 HTTP 报文中的 Java Applets。本例可以应用在本地用户需要访问远程网络服务的情况下。ASPF 配置的基本步骤如下：

```
#在 ASPF 路由器上配置允许防火墙
[Quidway] firewall enable
#配置访问控制列表 111，以拒绝所有 TCP 和 UDP 流量进入内部网络，ASPF 会为允许通过的流量创建
#临时的访问控制列表
[Quidway] acl number 111
[Quidway-acl-adv-111] rule deny
```

#创建 ASPF 策略，策略号为 1，该策略检测应用层的两个协议为 FTP 和 HTTP，在定义没有任何行为的情况下，这两个协议的超时时间为 3000s。

```
[Quidway] aspf-policy 1
[Quidway-aspf-policy-1] detect ftp aging-time 3000
[Quidway-aspf-policy-1] detect http aging-time 3000
[Quidway-aspf-policy-1] detect http java-list 1
#配置访问控制列表 1，以过滤来自站点 122.35.2.1 的 Java Applets
[Quidway] acl number 1
[Quidway-acl-basic-1] rule deny source 122.35.2.1 0
[Quidway-acl-basic-1] rule permit any
#在接口上应用 ASPF 策略
[Quidway-Serial1/0/0] firewall aspf 1 outbound
#在接口上应用访问控制列表 111
[Quidway-Serial1/0/0] firewall packet-filter 1 inbound
```

6.9 本章小结



防火墙技术
PIX防火墙配置
nameif
interface
ip address
nat
global
route
防火墙技术
包过滤技术
静态包过滤防火墙
动态包过滤防火墙
代理服务
应用级网关防火墙
电路级网关防火墙
防火墙体系结构
双重宿主主机体系结构
屏蔽主机体系结构
屏蔽子网体系结构
防火墙选择原则
应该是一个整体网络的保护者
必须能弥补其他操作系统的不足
应该为使用者提供不同平台的选择
能向使用者提供完善的售后服务
应该提供完整的安全检查功能
应该能实现IP转换
应该有双重DNS
应该具有查杀的功能
发展
第一代：包过滤防火墙
第二代：电路级网关防火墙
第三代：应用级网关防火墙
第四代：动态包过滤防火墙
第五代：自适应代理防火墙
概念
由软件和硬件组成的系统，它处于安全的网络和不安全的网络之间，根据系统管理员设置的访问控制规则，对数据流进行过滤
功能
建立一个集中的监视点
监视网络的安全性，并产生报警
网络地址转换
审计和记录Internet使用量
强化网络安全策略
功能局限性
对于绕开了防火墙的攻击行为，防火墙不能提供保护
防火墙对来自内部的威胁不能提供保护
防火墙不能对那些已经受到病毒感染的程序和文件的传输提供保护
分类
软硬件形式分类
软件防火墙
硬件防火墙
芯片级防火墙
过滤层次分类
包过滤防火墙
电路级网关防火墙
应用层网关防火墙
部署位置分类
边界防火墙
个人防火墙
混合式防火墙

6.10 习　　题

一、填空题

1. 防火墙按软硬件形式分类可以分为软件防火墙、硬件防火墙和(　　)。

2. 包过滤防火墙工作在 OSI 参考模型的网络层和(　　)。

3. 防火墙最简单的形式是(　　)。

4. 动态包过滤防火墙又称为(　　),它是在静态包过滤防火墙的基础上发展而来的。

5. (　　)必须为特定的应用编写特定的程序,这些程序的集合称为代理服务。

6. 双重宿主主机体系结构是围绕具有双重宿主的计算机而构建的,该计算机至少有(　　)个网络接口。

7. 在屏蔽子网体系结构中,用户把(　　)连接到周边网,这台主机便是与外界连接的主要入口。

二、选择题

1. 某公司申请到 5 个合法 IP 地址,要使公司的 20 台主机都能联网到因特网上,需要防火墙的(　　)技术。

A. 假冒 IP 地址的侦测　　B. 网络地址转换

C. 内容检查　　D. 基于地址的身份认证

2. 包过滤依据包的源地址、目的地址、传输协议来确定数据包的转发,它不能进行的操作为(　　)。

A. 禁止外部网络用户使用 FTP

B. 允许所有用户使用 HTTP 浏览因特网

C. 除了管理员可以从外部网络 telnet 内部网络外,其他用户都不可以

D. 只允许某台计算机通过 NNTP 发布新闻

3. 关于规则,以下描述错误的是(　　)。

A. 过滤器可以由多项规则组成

B. 根据规则顺序逐项匹配

C. 只有和当前规则不匹配时,才和后续规则进行匹配操作

D. 匹配结果与过滤器中的规则顺序无关

4. 下面关于个人防火墙特点的说法中,错误的是(　　)。

A. 个人防火墙可以抵挡外部攻击

B. 个人防火墙能够隐蔽个人计算机的 IP 地址等信息

C. 个人防火墙既可以对单机提供保护,也可以对网络提供保护

D. 个人防火墙占用一定的系统资源

5. 下面关于防火墙的描述中,正确的是(　　)。

A. 防火墙不会降低计算机网络系统的性能

B. 防火墙可以解决来自内部网络的攻击

C. 防火墙可以阻止感染病毒文件的传送

D. 防火墙对绕过防火墙的访问和攻击无能为力

6. 当某一服务器需要同时为内网用户和外网用户提供安全可靠的服务时,该服务器一般置于防火墙的(　　)。

A. 内部　　B. 外部

C. DMZ 区　　D. 以上选项都可以

7. 下面关于防火墙的说法中,正确的是(　　)。

A. 防火墙可以解决来自内部网络的攻击

B. 防火墙可以防止受病毒感染的文件传输

C. 防火墙会削弱计算机网络系统的性能

D. 防火墙可以防止错误配置引起的安全威胁

8. 包过滤技术防火墙在过滤数据包时,一般不关心(　　)。

A. 数据包的源地址　　B. 数据包的目的地址

C. 数据包的协议类型　　D. 数据包的内容

9. 以下(　　)不属于网络防火墙的类型。

A. 包过滤路由器　　B. 应用级网关

C. 电路级网关　　D. 堡垒主机

10. 关于防火墙,以下描述错误的是(　　)。

A. 不能防范内网内的恶意攻击

B. 不能防范针对面向连接协议的攻击

C. 不能防范病毒和内部驱动的木马

D. 不能防范针对防火墙开放端口的攻击

三、判断题

1. 防火墙一般采用"所有未被允许的就是禁止的"和"所有未被禁止的就是允许的"两个基本准则,其中前者的安全性要比后者高。

2. 包过滤防火墙一般工作在 OSI 参考模型的网络层和传输层,主要对 IP 分组和 TCP/UDP 的端口进行检测和过滤操作。

3. 当硬件配置相同时,代理防火墙对网络性能的影响比包过滤防火墙小。

4. 有些个人防火墙是一款独立的软件,而有些个人防火墙则融合在防病毒软件中使用。

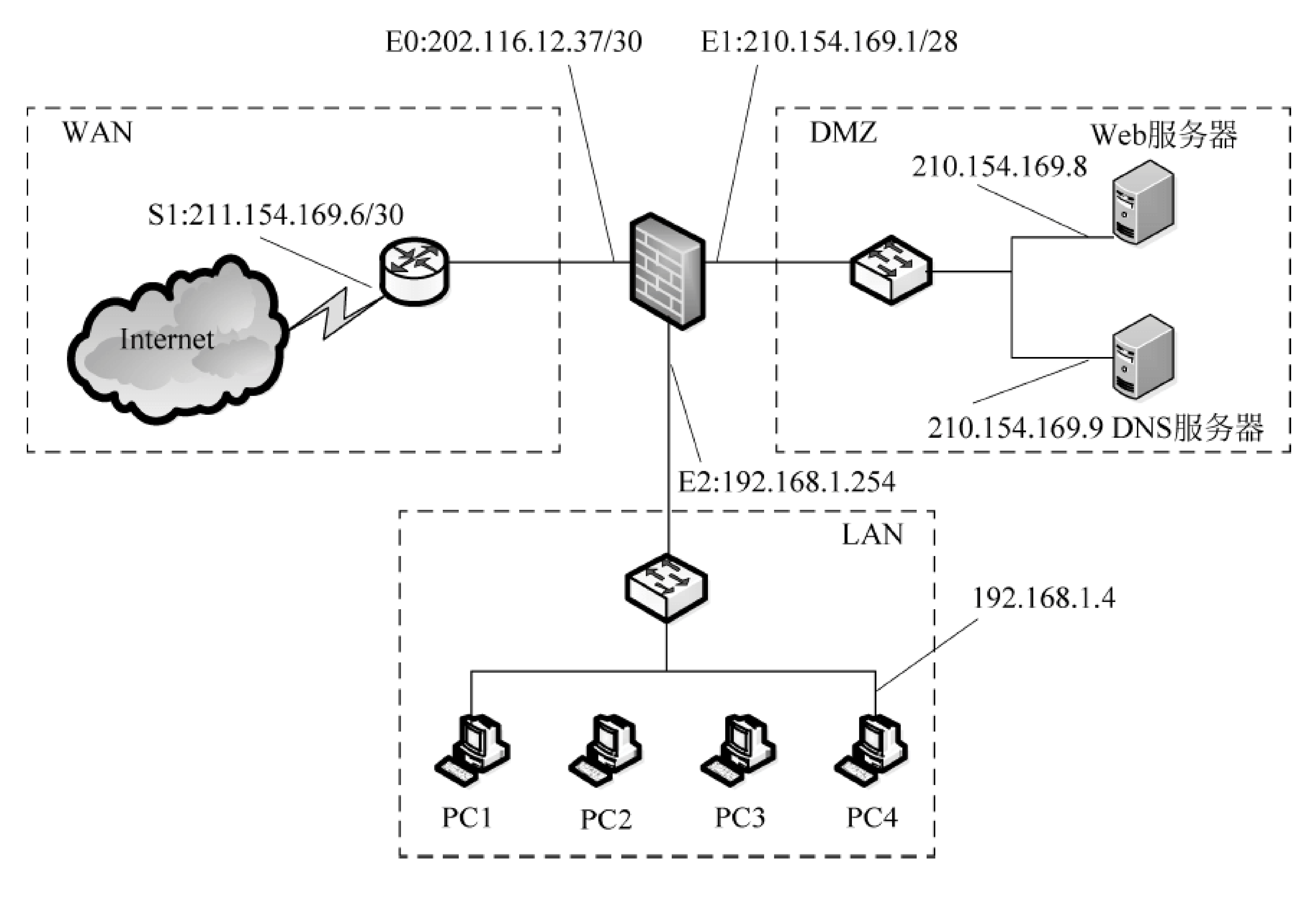
四、简答题

1. 防火墙具有哪些功能?

2. 防火墙的体系结构有哪些?

五、综合题

1. 某企业的网络安装防火墙的拓扑结构如下图所示。防火墙包过滤规则的默认策略为拒绝,下表给出防火墙的包过滤规则配置界面。请参考例子分别为下面两个需求配置相应的包过滤规则。



例：要求内网所有用户能使用浏览器访问 DMZ 区的 Web 服务器 210.156.169.8，如下表。

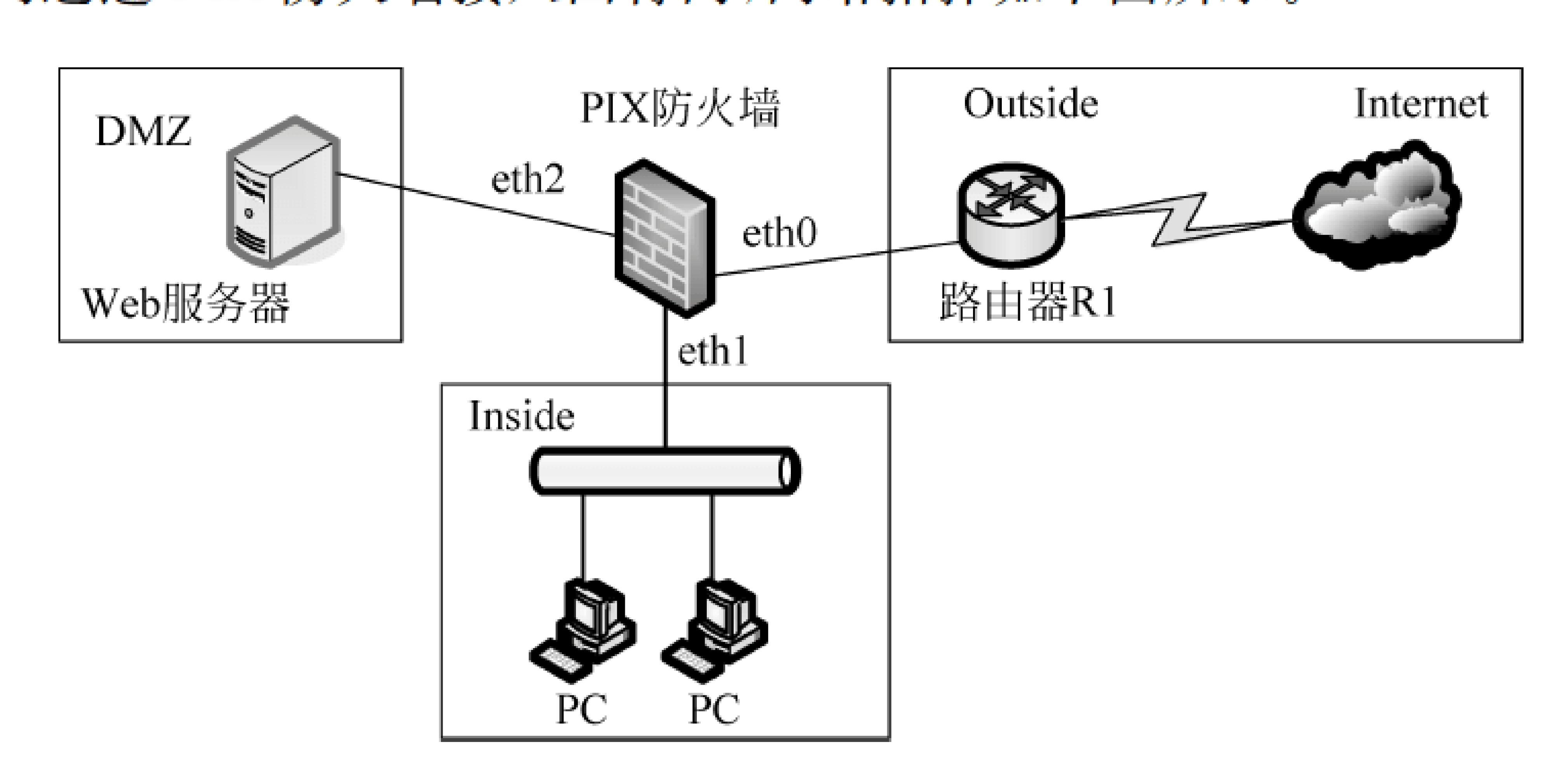
序号	策略	源地址	源端口	目的地址	目的端口	协议	方向
例	允许	192.168.1.0	any	210.154.169.8	80	TCP	E2→E1
(1)							
(2)							
(3)							

(1) 要求外网所有用户能使用 IE 浏览器访问 DMZ 区的 Web 服务器 210.156.169.8。

(2) 要求内网所有用户能使用 IE 浏览器访问外网的所有 Web 服务器。

(3) 禁止 PC3 访问地址为 210.156.169.8 的 Web 服务器。

2. 某公司通过 PIX 防火墙接入因特网，网络拓扑如下图所示。



在防火墙上利用 show 命令查询当前配置信息如下：

```
…
nameif eth0 outside security0
nameif eth1 inside security100
nameif eth2 dmz security40
…
```

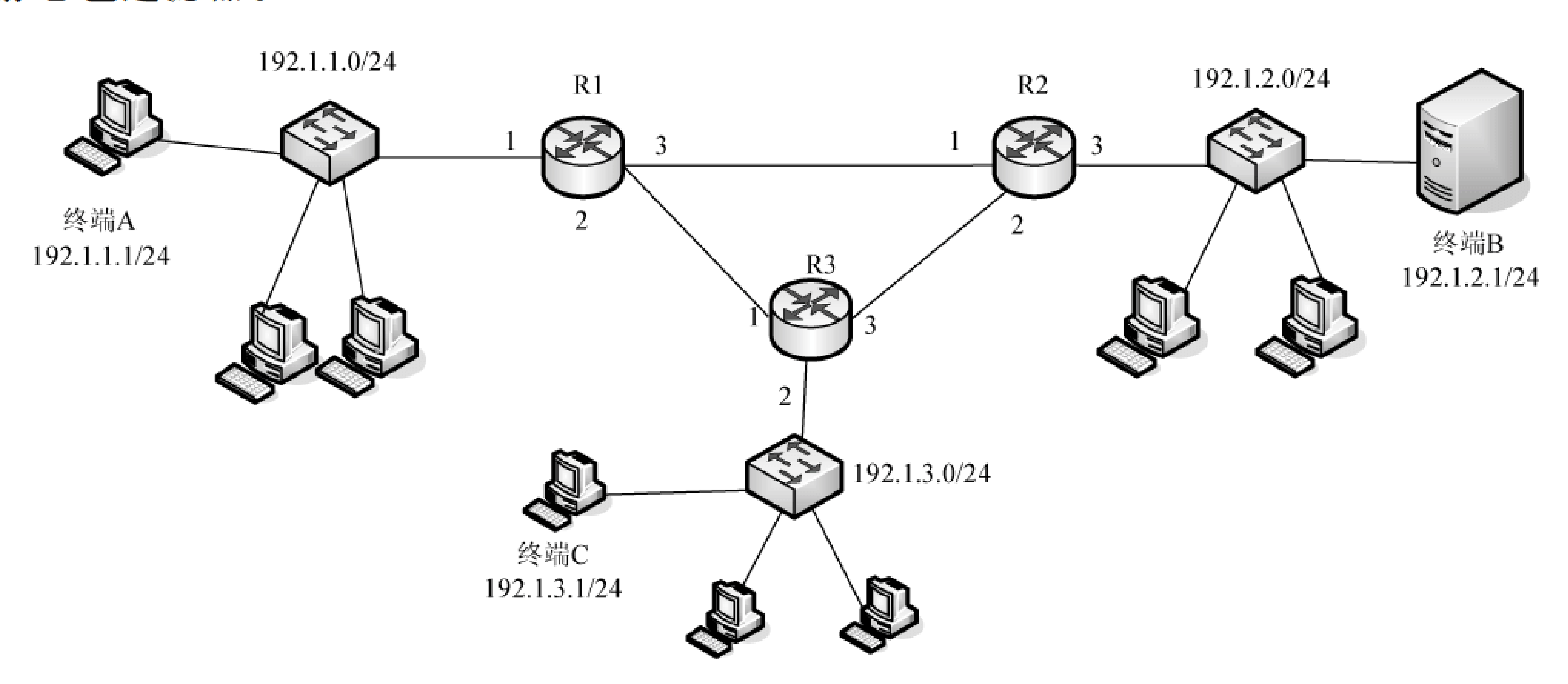
```
ip address outside 61.144.51.42   255.255.255.248
ip address inside 192.168.1.1     255.255.255.0
ip address dmz 10.10.0.1          255.255.255.0
…
global (outside) 1 61.144.51.46
nat (inside) 1 0.0.0.0 0.0.0.0
```

(1) 根据配置信息填写下表。

域　名　称	接口名称	IP 地址	IP 地址掩码
inside	eth1	①	255.255.255.0
outside	eth0	61.144.51.42	②
dmz	③	④	255.255.255.0

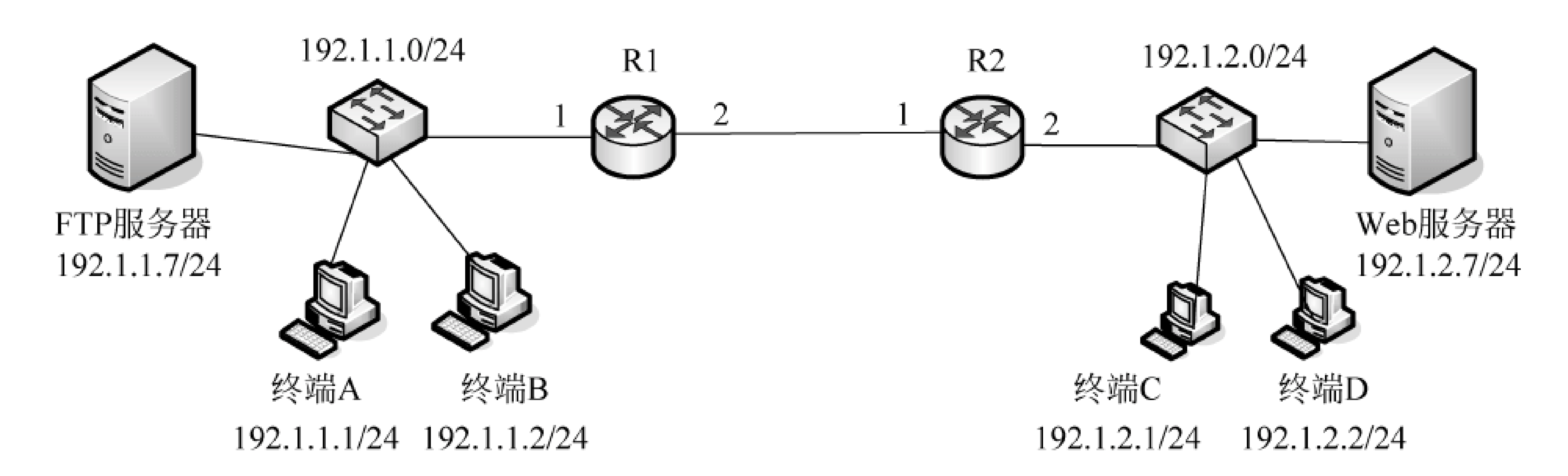
(2) 根据所显示的配置信息，由 inside 域发往因特网的 IP 分组在到达路由器 R1 时的源地址是什么？

3. 网络结构如下图所示，要求禁止终端 A、终端 B 和终端 C 之间相互通信，但允许这三个终端和其他终端相互通信，同时也允许其他终端之间相互通信，请填下表，给出需要配置的静态包过滤器。



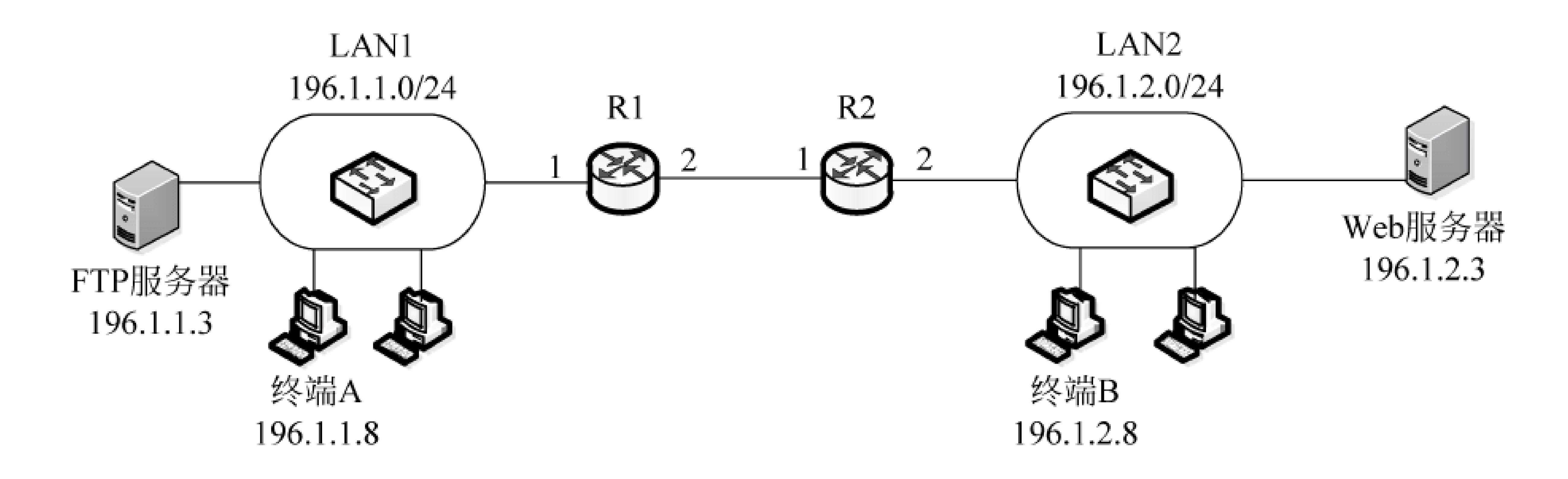
协　　议	源 IP	目的 IP	动　　作
路由器 R1 接口 1 输入方向			
IP			
IP			
IP			
路由器 R2 接口 3 输入方向			
IP			
IP			
IP			
路由器 R3 接口 2 输入方向			
IP			
IP			
IP			

4. 网络结构如下图所示。请填下表,要求实现只允许终端 A 发起访问 Web 服务器,终端 C 发起访问 FTP 服务器,禁止其他一切网络间通信的数据传输控件。



协议	源 IP	源端口	目的 IP	目的端口	动作
路由器 R1 接口 1 输入方向					
TCP					
TCP					
TCP					
IP					
路由器 R2 接口 2 输入方向					
TCP					
TCP					
TCP					
IP					

5. 网络结构如下图所示,如果只允许 LAN1 内终端访问 LAN2 内的 Web 服务器,禁止其他信息的传输,如何在路由器中设置静态包过滤,请填下表。



路由器 R1 接口 1 输入方向分组过滤

规则号	协议	源 IP 地址	目的 IP 地址	源端口号	目的端口号	动　　作
1						
2						

如果安全策略是“只允许经过终端 B 访问 FTP 服务器操作有关的 IP 分组，禁止经过路由器传输其他一切类型的 IP 分组”，如何设置路由器中静态包过滤，请填下表。

路由器 R1 接口 1 输出方向分组过滤

规则号	协议	源 IP 地址	目的 IP 地址	源端口号	目的端口号	动作
1						
2						
3						

第7章 入侵检测技术

【本章学习目标】

- 了解入侵检测的定义
- 理解入侵检测通用模型
- 了解入侵检测系统结构
- 了解入侵检测系统类型及优缺点
- 掌握异常检测与误用检测技术
- 掌握 Snort 入侵检测系统

7.1 入侵检测概述

7.1.1 入侵检测系统的概念

入侵是一个广义上的概念，是指任何非授权进入系统进行访问、威胁和破坏的行为。实施入侵的人通常称为入侵者或攻击者。

美国国家安全通信委员会(NSTAC)下属的入侵检测小组(IDSG)在1997年给出的关于“入侵检测”(Instruction Detection，ID)的定义是：入侵检测是对企图入侵、正在进行的入侵或已经发生的入侵行为进行识别的过程。入侵检测是继“防火墙”“信息加密”等传统安全保护方法之后的新一代安全保障技术。它监视计算机系统或网络中发生的事件，并对它们进行分析，以寻找危及信息保密性、完整性和可用性的入侵行为。

入侵检测系统(Instruction Detection System，IDS)是指对入侵行为自动进行检测、监控和分析的软件与硬件的组合系统，是一种自动监测信息系统内、外入侵事件的安全设备。它与其他网络安全设备的不同之处在于，IDS是一种积极主动的安全防护技术。

7.1.2 入侵检测系统的发展

入侵检测系统作为安全体系中一个重要环节，从实验室原型研究到推出商业化产品，再到走向市场获得广泛认同，已经走过了30多年的风雨坎坷路。

1. 概念的诞生

1980年4月，James P. Anderson 向美国空军提交了一份题为 *Computer Security Threat Monitoring and Surveillance*(计算机安全威胁监控与监视)的技术报告，第一次详细阐述了入侵检测的概念，并提出了一种对计算机系统风险和威胁的分类方法，以及利用审计跟踪数据监视入侵活动的思想。

2. 主机 IDS 研究

1984—1986 年，乔治敦大学的 Dorothy Denning 和 SRI/CSL（SRI 公司计算机科学实验室）的 Peter Neumann 研究出了一个实时入侵检测系统模型，取名为 IDES（入侵检测专家系统）。该模型由 6 个部分组成：主体、对象、审计记录、轮廓特征、异常记录、活动规则。它独立于特定的系统平台、应用环境、系统弱点以及入侵类型，为构建入侵检测系统提供了一个通用的框架。

1988 年，SRI/CSL 的 Teresa Lunt 等人改进了 Denning 的入侵检测模型，并成功开发了一个 IDES。该系统包含一个异常检测器和一个专家系统，分别用于统计异常模型的建立和基于规则的特征分析检测。该系统被认为是入侵检测研究中最有影响的一个系统，也是第一个在应用中运用了统计和基于规则两种技术的系统。

3. 网络 IDS 研究

1990 年是入侵检测系统发展的一个分水岭。这一年，加州大学戴维斯分校的 L. T. Heberlein 等人开发了网络安全监视器（Network Security Monitor，NSM）。该系统第一次直接将网络流作为审计数据来源，因而可以在不将审计数据转换成统一格式的情况下监控异常主机。从此以后，入侵检测系统发展史翻开了新的一页，基于网络的入侵检测系统和基于主机的入侵检测系统两大阵营正式形成。

4. 主机 IDS 和网络 IDS 的集成

莫里斯蠕虫事件发生之后，网络安全才真正引起了人们的高度重视。美国空军、国家安全局和能源部共同资助空军密码支持中心、劳伦斯利弗摩尔国家实验室、加州大学戴维斯分校、Haystack 实验室，开展对分布式入侵检测系统（DIDS）的研究，将基于主机的和基于网络的检测方法集成在一起。

从 20 世纪 90 年代至今，入侵检测系统的研发呈现出百家争鸣的繁荣局面，并在智能化和分布式两个方向取得了长足性的进展。目前 SRI/CSL、普渡大学、加州大学等机构在这些方面的研究代表了当前的最高水平。

7.2 入侵检测系统结构

7.2.1 入侵检测系统通用模型

对于入侵检测框架的研究比较有名的成果是入侵检测数据交换格式（Intrusion Detection Exchange Format，IDEF）和通用入侵检测框架（Common Intrusion Detection Framework，CIDF）。

IDEF 是由 IETF 的入侵检测工作组（Intrusion Detection Working Group，IDWG）负责建立的入侵检测数据交换标准。

CIDF 标准由美国加州大学戴维斯分校的安全实验室提出并完成。CIDF 是一套规范，定义了 IDS 表达入侵检测信息的标准语言，用来表示系统事件、分析结果和响应指标，把入侵检测系统从逻辑上分为各个面向任务的组件，定义了 IDS 组件之间的通信协议。CIDF 的文档由 4 部分组成，包括体系结构、规范语言、内部通信和程序接口。

CIDF 的体系结构文档中说明了一个 IDS 的通用模型。如图 7-1 所示，CIDF 将入侵检

测系统所要分析的数据统称为事件(event)。它将入侵检测系统分为事件产生器、事件分析器、响应单元和事件数据库4个组件。

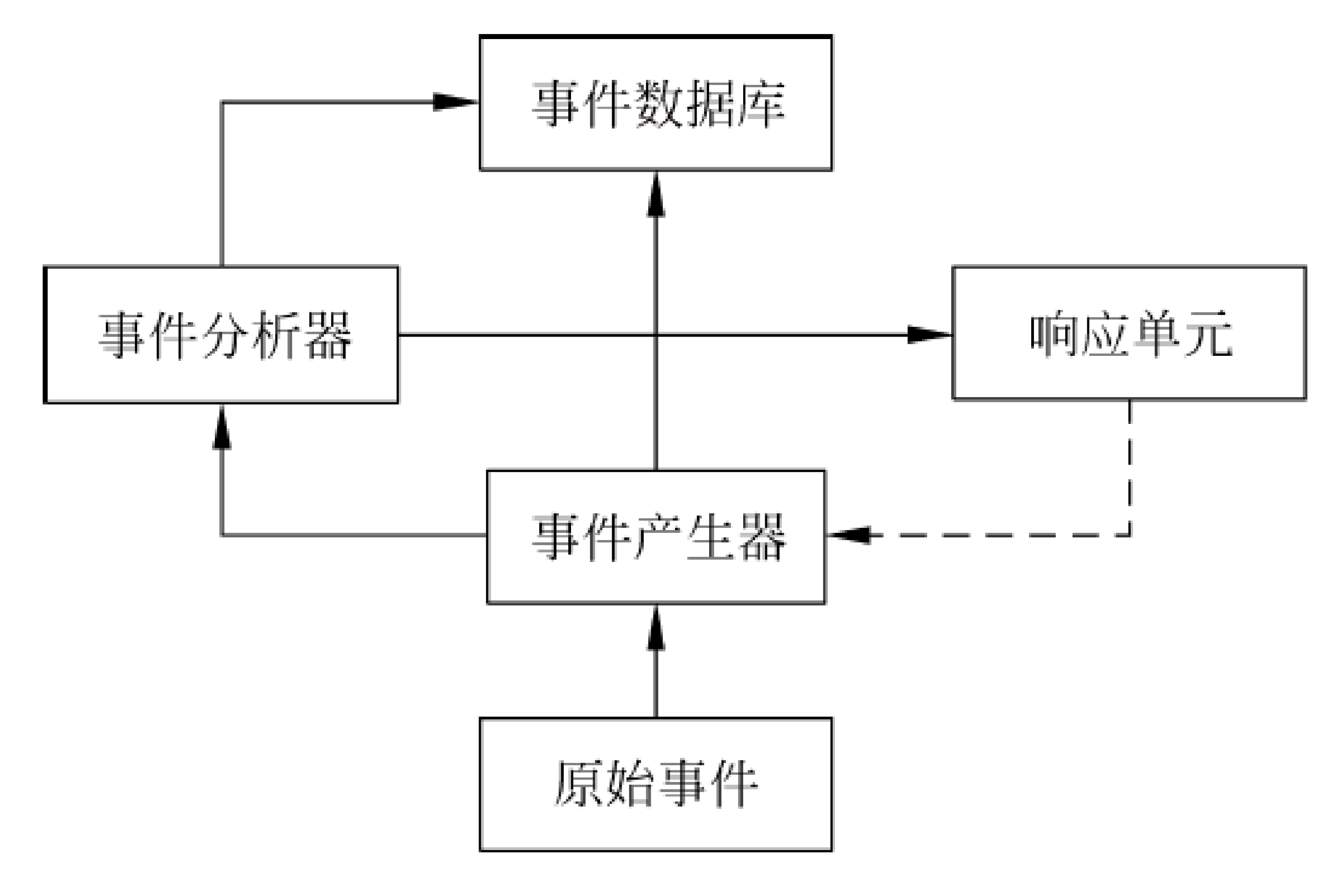


图7-1 CIDF通用模型

1. 事件产生器

事件产生器负责从整个计算环境中获取事件。事件可以是从网络数据包或系统日志等途径获取的数据,一般将其保存到数据库中。

2. 事件分析器

事件分析器负责分析事件产生器搜集的数据,发现非法的、具有潜在危险的、异常的数据,即通知响应单元做出入侵响应;另外它还要对数据库保存的数据做定期统计分析,做阶段性的异常数据详细分析。

3. 响应单元

响应单元在事件分析器发现具有入侵迹象的异常数据后开始工作,它可以中止进程、切断连接、改变属性,或只是做简单的报警。

4. 事件数据库

事件数据库负责存储事件产生器、事件分析器获取的数据和分析的结果。

7.2.2 入侵检测系统结构概述

入侵检测系统是监测网络和系统以发现违反安全策略事件的过程。根据CIDF框架模型,可以知道IDS一般包括三个部分:采集模块、分析模块和管理模块。

1. 采集模块

采集模块主要用来信息收集,供入侵检测系统进行分析。信息收集的内容包括系统、网络、数据及用户活动的状态和行为。通常需要在计算机网络系统中的若干不同关键点(不同网段和不同主机)收集信息,这除了尽可能扩大检测范围的原因外,还有一个重要的原因就是从一个源来的信息有可能看不出疑点,但从几个源来的信息的不一致性却是可疑行为或入侵的最好标识。

入侵检测在很大程度上依赖于收集信息的可靠性和正确性,因为入侵者经常替换软件以搞混和移走这些信息,如替换被程序调用的子程序、库和其他工具,所以,有必要利用已知的真正的和精确的软件来报告这些信息。入侵者对系统的修改可能使系统功能失常但看起来跟正常的一样。这需要保证用来检测网络系统的软件的完整性,特别是入侵检测系统软

件本身应具有相当强的坚固性，防止被篡改而收集到错误的信息。

入侵检测利用的信息一般来自以下 4 个方面。

(1) 系统和网络日志。如果不知道入侵者在系统上做了什么，那是不可能发现入侵的。日志提供了当前系统的细节，记录哪些系统被攻击了，哪些系统被攻破了。因此，充分利用系统和网络日志文件信息是检测入侵的必要条件。日志中包含发生在系统和网络上的不寻常和不期望活动的证据，这些证据可以指出有人正在入侵或已成功入侵了系统。通过查看日志文件，能够发现已成功地入侵或入侵企图，并很快地启动相应的应急响应程序。日志文件中记录了各种行为类型，每种类型又包含不同的信息，例如记录“用户活动”类型的日志，就包含登录、用户 ID 改变、用户对文件的访问、授权和认证信息等内容。很显然，对用户活动来讲，不正常的或不期望的行为就是重复登录失败、登录到不期望的位置以及非授权的企图访问重要文件等。由于日志的重要性，所有重要的系统都应定期做日志，而且日志应被定期保存和备份，因为不知何时会需要它。许多专家建议定期向一个中央日志服务器上发送所有日志，而这个服务器使用一次性写入的介质来保存数据，这样就避免了攻击者篡改日志。系统本地日志与发到一个远端系统保存的日志提供了冗余和一个额外的安全保护层。现在两个日志可以互相比较，任何的不同均显示了系统的异常。

(2) 目录和文件中的不期望的改变。网络环境中的文件系统包含很多软件和数据文件，包含重要信息的文件和私有数据文件经常是攻击者修改或破坏的目标。目录和文件中的不期望的改变(包括修改、创建和删除)，特别是那些正常情况下限制访问的，很可能就是一种入侵产生的指示和信号。攻击者经常替换、修改和破坏他们获得访问权的系统上的文件，同时为了隐藏系统中他们的表现及活动痕迹，都会尽力去替换系统程序或修改系统日志文件。

(3) 程序执行中的不期望行为。网络系统上的程序执行一般包括操作系统、网络服务、用户启动的程序和特定目的的应用，如数据库服务器。每个在系统上执行的程序由一个到多个进程来实现。每个进程在具有不同权限的环境中执行，这种环境控制着进程可访问的系统资源、程序和数据文件等。一个进程的执行行为由它运行时执行的操作来表现，操作执行的方式不同，它利用的系统资源也就不同。操作包括计算、文件传输和其他进程，以及与网络间其他进程的通信。一个进程出现了不期望的行为表明攻击者可能正在入侵系统。攻击者可能会将程序或服务的运行分解，从而导致它失败，或者是以非用户或管理员意图的方式操作。

(4) 物理形式的入侵信息。这包括两个方面的内容：一是未授权的对网络硬件的连接；二是对物理资源的未授权访问。入侵者会想方设法去突破网络的周边防卫，如果他们能够在物理上访问内部网，就能安装他们自己的设备和软件。由此入侵者就可以知道网上的由用户加上去的不安全(未授权)设备，然后利用这些设备访问网络。

2. 分析模块

分析模块完成对数据的解析，给出怀疑值或做出判断。一般通过三种技术手段进行分析：模式匹配、统计分析和完整性分析。其中前两种方法用于实时的入侵检测，而完整性分析则用于事后分析。

(1) 模式匹配。模式匹配就是将收集到的信息与已知的网络入侵和系统误用模式数据库进行比较，从而发现违背安全策略的行为。该过程可以很简单(如通过字符串匹配以寻找一个简单的条目或指令)，也可以很复杂(如利用正规的数学表达式来表示安全状态的变化)。一般

来讲，一种进攻模式可以用一个过程（如执行一条指令）或一个输出（如获得权限）来表示。该方法的一大优点是只需收集相关的数据集合，显著减少系统负担，且技术已相当成熟。它与病毒防火墙采用的方法一样，检测准确率和效率都相当高。但是该方法存在的弱点是需要不断地升级以对付不断出现的黑客攻击手法，不能检测到从未出现过的黑客攻击手段。

（2）统计分析。统计分析方法首先给系统对象（如用户、文件、目录和设备等）创建一个统计描述，统计正常使用时的一些测量属性（如访问次数、操作失败次数和延时等）。测量属性的平均值将被用来与网络、系统的行为进行比较，任何观察值在正常值范围之外时，就认为有入侵发生。例如，统计分析可能标识一个不正常行为，因为它发现一个在晚 8 点至早 6 点没有登录的账户却在凌晨两点试图登录。其优点是可检测到未知的入侵和更为复杂的入侵，缺点是误报、漏报率高，且不适应用户正常行为的突然改变。具体的统计分析方法如基于专家系统的、基于模型推理的和基于神经网络的分析方法，目前正处于研究热点和迅速发展之中。

（3）完整性分析。完整性分析主要关注某个文件或对象是否被更改，这经常包括文件和目录的内容及属性，它在发现被更改的应用程序方面特别有效。完整性分析使用消息摘要函数（例如 MD5），它能识别甚至是微小的变化。其优点是不管模式匹配方法和统计分析方法能否发现入侵，只要是成功的攻击导致了文件或其他对象的任何改变，它都能够发现。它的缺点是一般以批处理方式实现，不用于实时响应。尽管如此，完整性检测方法还应该是网络安全产品的必要手段之一。如可以在每一天的某个特定时间内开启完整性分析模块，对网络系统进行全面的扫描检查。

3. 管理模块

管理模块主要功能是做决策和响应。入侵检测响应方式分为主动响应和被动响应。

目前，主动响应系统还比较少，即使做出主动响应，一般也都是断开可疑攻击的网络连接，或是阻塞可疑的系统调用，若失败，则终止该进程。但由于系统暴露于拒绝服务攻击下，这种防御一般也难以实施。主动响应系统可以分为对被攻击系统实施控制和对攻击系统实施控制的系统。

（1）对被攻击系统实施控制（防护）。它通过调整被攻击系统的状态，阻止或减轻攻击影响，例如断开网络连接、增加安全日志、阻止可疑进程等。

（2）对攻击系统实施控制（反击）。这种系统多被军方所重视和采用。

被动响应型系统只会发出报警通知，将发生的不正常情况报告给管理员，本身并不试图降低所造成的破坏，更不会主动地对攻击者采取反击行动。

7.3 入侵检测系统类型

根据入侵检测系统的检测对象和工作方式的不同，可将入侵检测系统分为两大类：基于主机的入侵检测系统（Host-based IDS，HIDS）和基于网络的入侵检测系统（Network-based IDS，NIDS）。

7.3.1 基于主机的入侵检测系统

基于主机的入侵检测系统是在主机或操作系统上检查有关信息来探测入侵行为。这种入侵检测系统通过系统调用、审计日志和错误信息等对主机进行分析。一个典型的基于主

机的入侵检测系统部署如图 7-2 所示。

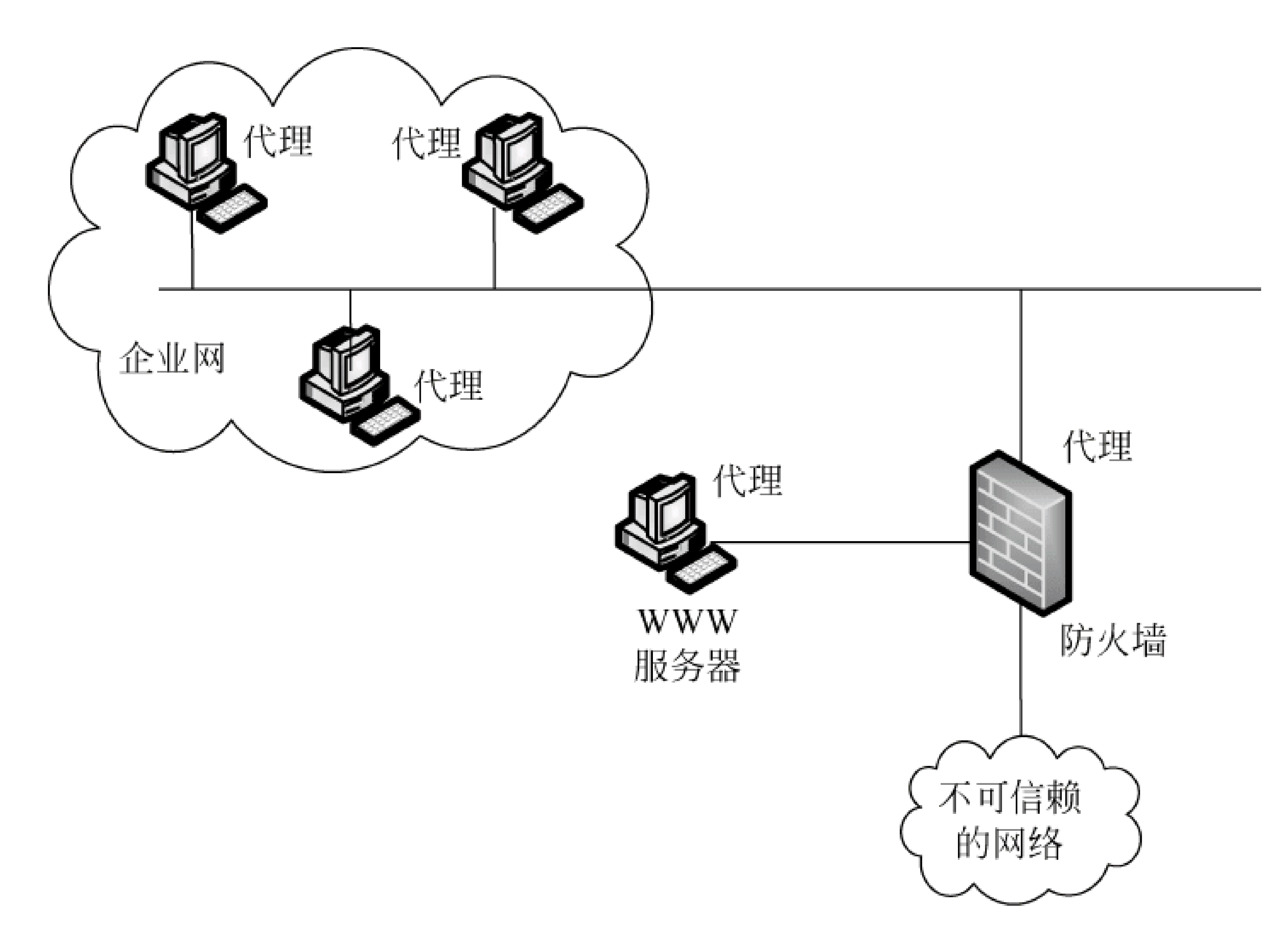


图 7-2 基于主机的入侵检测系统部署

基于主机的入侵检测系统通常是安装在被重点检测的主机上，主要是对该主机的网络实时连接以及系统审计日志进行智能分析和判断。如果其主机活动十分可疑（特征或违反统计规律），入侵检测系统就会采取相应措施。

基于主机的入侵检测系统使用验证记录，并发展了精密的可迅速做出响应的检测技术。通常基于主机的入侵检测系统可监测系统、事件和 Window NT 下的安全记录以及 UNIX 环境下的系统记录。当有文件发生变化时，入侵检测系统将新的记录条目与攻击标记相比较，看它们是否匹配。如果匹配，系统就会向管理员报警并向别的目标报告，以采取措施。

基于主机的入侵检测系统在发展过程中融入了其他技术。对关键系统文件和可执行文件的入侵检测的一个常用方法，是通过定期检查校验和来进行的，以便发现意外的变化。反应的快慢与轮询间隔的频率有直接的关系。许多系统都是监听端口的活动，并在特定端口被访问时向管理员报警。这类检测方法将基于网络的入侵检测的基本方法融入基于主机的检测环境中。

尽管基于主机的入侵检测系统不如基于网络的入侵检测系统快捷，但它确实具有基于网络的入侵检测系统无法比拟的优点。

1. 基于主机的入侵检测系统优点

（1）确定攻击是否成功。由于基于主机的入侵检测系统使用已发生事件的信息，它们可以比基于网络的入侵检测系统更加准确地判断攻击是否成功。在这方面，基于主机的入侵检测系统是基于网络的入侵检测系统完美补充，网络部分可以尽早提供警告，主机部分可以确定攻击成功与否。

（2）监视特定的系统活动。基于主机的入侵检测系统监视用户和访问文件的活动，包括文件访问、改变文件权限、试图建立新的可执行文件并且/或者试图访问特殊的设备。如基于主机的入侵检测系统可以监督所有用户的登录及下线情况，以及每位用户在连接到网络以后的行为。对于基于网络的系统要做到这个程度是非常困难的。基于主机技术还可监

视只有管理员才能实施的非正常行为。操作系统记录了任何有关用户账号的增加、删除、更改的情况，一旦改动发生，基于主机的入侵检测系统就能检测到这种不适当的改动。基于主机的入侵检测系统还可审计能影响系统记录的校验措施的改变，基于主机的系统可以监视系统文件和可执行文件的改变，系统能够查出那些欲改写重要系统文件或者安装特洛伊木马或后门的尝试并将它们中断，而基于网络的入侵检测系统有时会查不到这些行为。

(3) 能够检查到基于网络的系统检查不出的攻击。基于主机的系统可以检测到那些基于网络的系统察觉不到的攻击。如来自主要服务器键盘的攻击不经过网络，所以可以躲开基于网络的入侵检测系统。

(4) 适用被加密的和交换的环境。交换设备可将大型网络分成许多的小型网络部件加以管理，所以从覆盖足够大的网络范围的角度出发，很难确定配置基于网络的入侵检测系统的最佳位置。业务映射和交换机上的管理端口有助于此，但这些技术有时并不适用。基于主机的入侵检测系统可安装在所需的重要主机上，在交换的环境中具有更高的能见度。某些加密方式也向基于网络的入侵检测发出了挑战。由于加密方式位于协议堆栈内，所以基于网络的系统可能对某些攻击没有反应，基于主机的入侵检测系统没有这方面的限制，当操作系统及基于主机的系统看到即将到来的业务时，数据流已经被解密了。

(5) 近于实时的检测和响应。尽管基于主机的入侵检测系统不能提供真正实时的反应，但如果应用正确，反应速度可以非常接近实时。老式系统利用一个进程在预先定义的间隔内检查登记文件的状态和内容，与旧式系统不同，基于主机的系统采用中断指令，新的记录可被立即处理，显著减少了从攻击验证到做出响应的时间。在从操作系统做出记录到基于主机的系统得到辨识结果之间的这段时间是一段延迟，但大多数情况下，在破坏发生之前，系统就能发现入侵者，并阻止他的攻击。

(6) 不要求额外的硬件设备。基于主机的入侵检测系统存在于现行网络结构之中，包括文件服务器，Web 服务器及其他共享资源。这些使得基于主机的系统效率很高。因为它们不需要在网络上另外安装登记、维护及管理的硬件设备。

(7) 系统花费更加低廉。基于网络的入侵检测系统比基于主机的入侵检测系统要昂贵得多。

2. 基于主机的入侵检测系统缺点

(1) 主机入侵检测系统安装在我们需要保护的设备上，如需要保护一个数据库服务器时，就要在服务器上安装入侵检测系统，但这会降低应用系统的效率。此外，它也会带来一些额外的安全问题，安装了主机入侵检测系统后，将安全管理员本无权访问的服务器变成他可以访问的了。

(2) 主机入侵检测系统依赖于服务器固有的日志与监视能力。如果服务器没有配置日志功能，则必须重新配置，这将会给运行中的业务系统带来不可预见的性能影响。

(3) 全面部署主机入侵检测系统代价较大，企业中很难将所有主机用主机入侵检测系统保护，只能选择部分主机保护。那些未安装主机入侵检测系统的主机将成为保护的盲点，入侵者可利用这些主机达到攻击目标。

(4) 主机入侵检测系统除了监测自身的主机以外，根本不监测网络上的情况。对入侵行为的分析的工作量将随着主机数目增加而增加。

7.3.2 基于网络的入侵检测系统

基于网络的入侵检测系统对数据包进行分析以探测针对网络的攻击。这种入侵检测系统嗅探网络数据包,并将数据流与已知入侵行为的特征进行比较。一个典型的基于网络的入侵检测系统部署如图 7-3 所示。

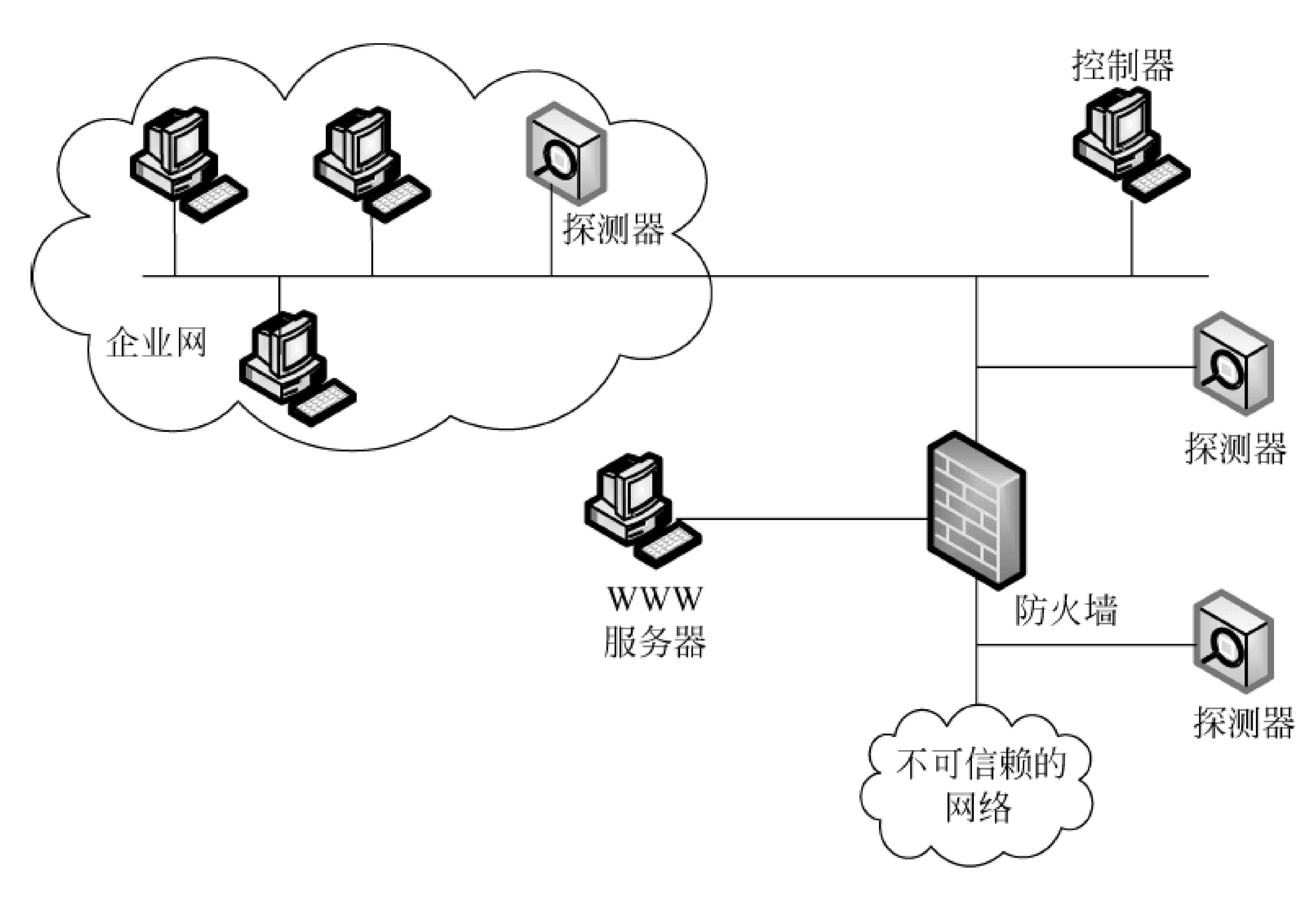


图 7-3　基于网络的入侵检测系统部署

基于网络的入侵检测系统使用原始网络包作为数据源。基于网络的入侵检测系统通常利用一个运行在随机模式下的网络适配器来实时监视并分析通过网络的所有通信业务。它的攻击辨识模块通常使用 4 种常用技术来识别攻击标志：模式、表达式或字节匹配；频率或穿越阀值；低级事件的相关性；统计学意义上的非常规现象检测。

一旦检测到了攻击行为,入侵检测系统的响应模块就提供多种选项以通知、报警并对攻击采取相应的反应。反应因系统而异,但通常都包括通知管理员、中断连接并且/或为法庭分析和证据收集而做的会话记录。

1. 基于网络的入侵检测系统优点

(1) 拥有成本较低。基于网络的入侵检测系统可在几个关键访问点上进行策略配置,以观察发往多个系统的网络通信。所以它不要求在许多主机上装载并管理软件。由于需监测的点较少,因此对于一个用户来说,拥有成本很低。

(2) 检测基于主机的系统漏掉的攻击。基于网络的入侵检测系统检查所有包的头部从而发现恶意的和可疑的行动迹象。基于主机的入侵检测系统无法查看包的头部,所以它无法检测到这一类型的攻击。例如,许多来自于 IP 地址的拒绝服务型和碎片型攻击只能在它们经过网络时,在基于网络的入侵检测系统中通过实时监测包流而被发现。基于网络的入侵检测系统可以检查有效负载的内容,查找用于特定攻击的指令或语法。如通过检查数据包有效负载可以查到黑客软件,而使正在寻找系统漏洞的攻击者毫无察觉。由于基于主机的系统不检查有效负载,所以不能辨认有效负载中所包含的攻击信息。

(3) 攻击者不易转移证据。基于网络的入侵检测系统使用正在发生的网络通信进行实时

攻击的检测，所以攻击者无法转移证据。被捕获的数据不仅包括攻击的方法，而且还包括可识别的入侵者身份及对其进行起诉的信息。许多入侵者都熟知审计记录，他们知道如何操纵这些文件掩盖他们的入侵痕迹，来阻止需要这些信息的基于主机的入侵检测系统去检测入侵。

(4) 实时检测和响应。基于网络的入侵检测系统可以在恶意及可疑的攻击发生的同时将其检测出来，并做出更快的通知和响应。例如，一个基于 TCP 的对网络进行的拒绝服务攻击可以通过将基于网络的入侵检测系统发出 TCP 复位信号，在该攻击对目标主机造成破坏前将其中断。而基于主机的系统只有在可疑的登录信息被记录下来以后才能识别攻击并做出反应，这时关键系统可能早就遭到了破坏，或是运行基于主机的入侵检测系统的系统已被摧毁。实时入侵检测系统可根据预定义的参数做出快速反应，这些反应包括将攻击设为监视模式以收集信息，立即阻止攻击等。

(5) 检测未成功的攻击和不良意图。基于网络的入侵检测系统增加了许多有价值的数据，以判别不良意图。即便防火墙可以正在拒绝这些尝试，位于防火墙之外的基于网络的入侵检测系统可以查出躲在防火墙后的攻击意图。基于主机的系统无法查到未攻击到防火墙内主机的未遂攻击，而这些丢失的信息对于评估和优化安全策略是至关重要的。

(6) 操作系统无关性。基于网络的入侵检测系统作为安全监测资源，与主机的操作系统无关。与之相比，基于主机的系统必须在特定的、没有遭到破坏的操作系统中才能正常工作，生成有用的结果。

2. 基于网络的入侵检测系统缺点

(1) 网络入侵检测系统只检测它直接连接网段的通信，不能检测在不同网段的网络包，在使用交换以太网的环境中会出现监测范围的局限。安装多台网络入侵检测系统的传感器会使部署整个系统的成本大大增加。

(2) 网络入侵检测系统为了性能目标通常采用特征检测的方法，它可以检测出一些普通的攻击，而很难实现一些复杂的需要大量计算与分析时间的攻击检测。

(3) 网络入侵检测系统可能会将大量的数据传回分析系统中。在一些系统中监听特定的数据包会产生大量的分析数据流量。一些系统在实现时采用一定方法来减少回传的数据量，对入侵判断的决策由传感器实现，而中央控制台成为状态显示与通信中心，不再作为入侵行为分析器。这样系统中的传感器协同工作能力较弱。

(4) 网络入侵检测系统处理加密的会话过程较困难。目前通过加密通道的攻击尚不多，但随着 IPv6 的普及，这个问题会越来越突出。

基于主机和基于网络的入侵检测都有其优势和劣势，两种方法互为补充。真正有效的入侵检测系统应将二者结合起来。

7.4 入侵检测技术

入侵检测系统的检测分析技术主要分为两大类：异常检测技术和误用检测技术。

7.4.1 异常检测技术

1. 异常检测技术基本原理

异常检测技术又称基于行为的入侵检测技术，用来识别主机或网络的异常行为。它假

设攻击与正常的(合法的)活动有明显的差异。异常检测首先收集一段时间操作活动的历史数据,再建立代表主机、用户或网络连接的正常行为描述,然后收集事件数据并使用一些不同的方法来决定所检测到的事件活动是否偏离了正常行为模式,从而判断是否发生了入侵。异常检测模型的结构如图7-4所示。

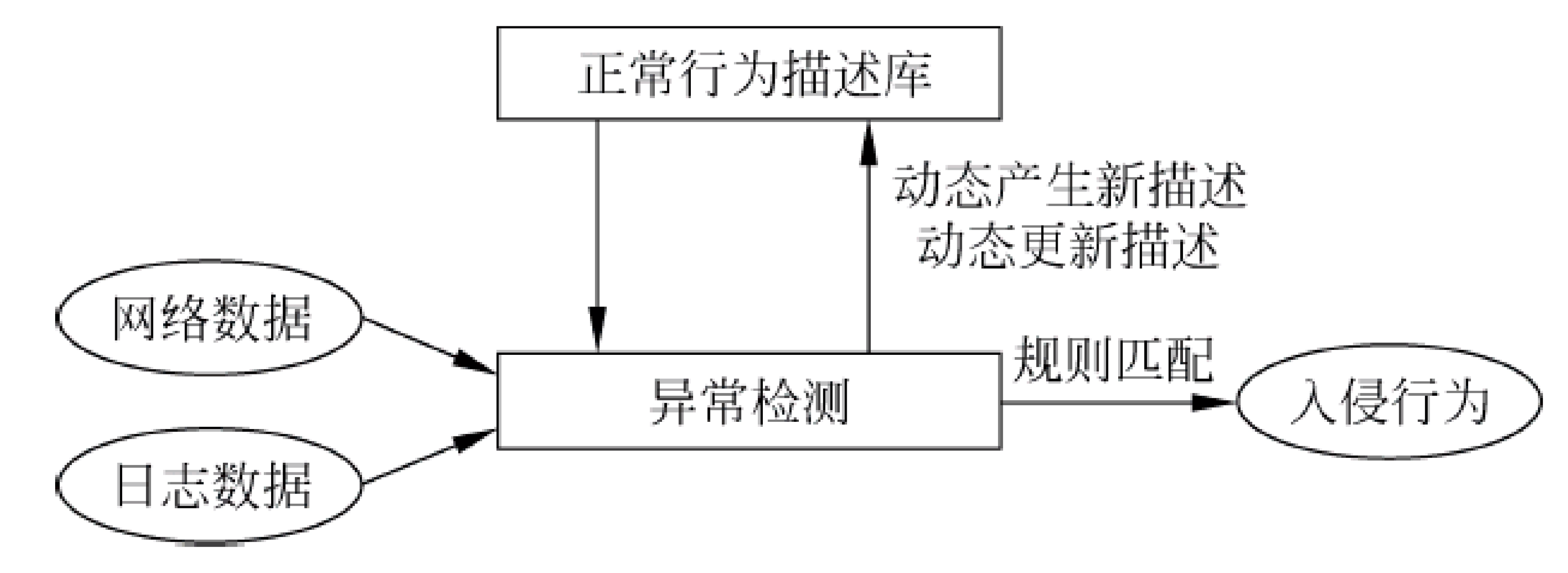


图7-4　异常检测模型的结构

2. 异常检测基本方法

异常检测是一个"学习正常,发现异常"的过程,它的主要特点体现在学习过程中,可以借鉴其他领域的方法来完成用户行为的学习和异常的检测。其主要的异常检测方法有:概率统计方法、神经网络方法、免疫方法等。

1)基于概率统计的检测

基于概率统计的检测技术是异常入侵检测中最常用的技术,它对用户历史行为建立模型。根据该模型,当入侵检测系统发现有可疑的用户行为发生时就保持跟踪,并监视和记录该用户的行为。

斯坦福国际研究院(Stanford Research Institute,SRI)研制开发的IDES是一个典型的实时监测系统。IDES能根据用户以前的历史行为生成每个用户的历史行为记录库,并能自适应地学习被检测系统中每个用户的行为习惯。当某个用户改变其行为习惯时,这种异常就被检测出来。这种系统具有固有的弱点,例如,用户的行为非常复杂,因而要想准确地匹配一个用户的历史行为和当前行为是非常困难的。这种方法的一些假设是不准确或不贴切的,容易造成系统误报、错报或漏报。

在这种实现方法中,检测器首先根据用户对象的动作为每一个用户建立一个用户特征表,通过比较当前特征和已存储的以前特征判断是否为异常行为。用户特征表需要根据审计记录情况不断加以更新。在SRI的IDES中给出了一个特征简表的结构:{变量名,行为描述,例外情况,资源使用,时间周期,变量类型,阈值,主体,客体,特征值},其中,变量名、主体、客体唯一确定了特征简表,特征值由系统根据审计数据周期产生。这个特征值是所有有悖于用户特征的异常程度值的函数。

这种方法的优越性在于能应用成熟的概率统计理论,不足之处在于:统计检测对于事件发生的次序不敏感,完全依靠统计理论,可能会漏掉那些利用彼此相关联事件的入侵行为。定义判断入侵的阈值比较困难,阈值太高则误检率提高,阈值太低则漏检率提高。

2)基于神经网络的检测

基于神经网络的检测技术的基本思想是用一系列信息单元训练神经单元,在给定一个输入后,就可能预测出输出。它是对基于概率统计的检测技术的改进,主要克服了传统的统计分析技术的一些问题。

基于神经网络的模块将当前命令和刚过去的 W 个命令组成了网络的输入，其中 W 是神经网络预测下一个命令时所包含的过去命令集的大小。根据用户的代表性命令序列训练网络后，该网络就形成了相应的用户特征表。网络对下一事件的预测错误率在一定程度上反映了用户行为的异常程度。这种方法的优点在于能够更好地处理原始数据的随机特征，即不需要对这些数据做任何统计假设并有较好的抗干扰能力；缺点是网络的拓扑结构及各元素的权值很难确定，命令窗口的 W 值也很难选取。窗口太大，网络效率降低；窗口太小，网络输出不理想。

目前，神经网络技术提出了对基于传统统计技术的攻击检测方法的改进方向，但尚不十分成熟，所以传统的统计方法仍继续发挥作用，仍然能为发现用户的异常行为提供相当有参考价值的信息。

3）基于免疫的检测

基于免疫的检测技术是将自然免疫系统的某些特征运用到网络系统中，使整个系统具有适应性、自我调节性、可扩展性。人的免疫系统成功地保护人体不受各种抗原和组织的侵害，这个重要特征吸引了许多计算机安全专家和人工智能专家。通过学习免疫专家的研究成果，计算机专家提出了计算机免疫系统。在许多传统的网络安全系统中，每个目标都将它的系统日志和收集到的信息传送给相应的服务器，由服务器分析整个日志和信息，判断是否发生恶意入侵。基于免疫的入侵检测系统运用计算免疫的多层性、分布性、多样性等特性设置动态代理，实施分层检测和响应机制。

7.4.2 误用检测技术

1. 误用检测技术基本原理

误用检测技术又称基于知识的检测技术。它假设所有入侵行为和手段都能够表达为一种模式或特征，并对已知的入侵行为和手段进行分析，提取检测特征，构建攻击模式或攻击签名，通过系统当前状态与攻击模式或攻击签名的匹配判断入侵行为。误用检测模式的结构如图 7-5 所示。

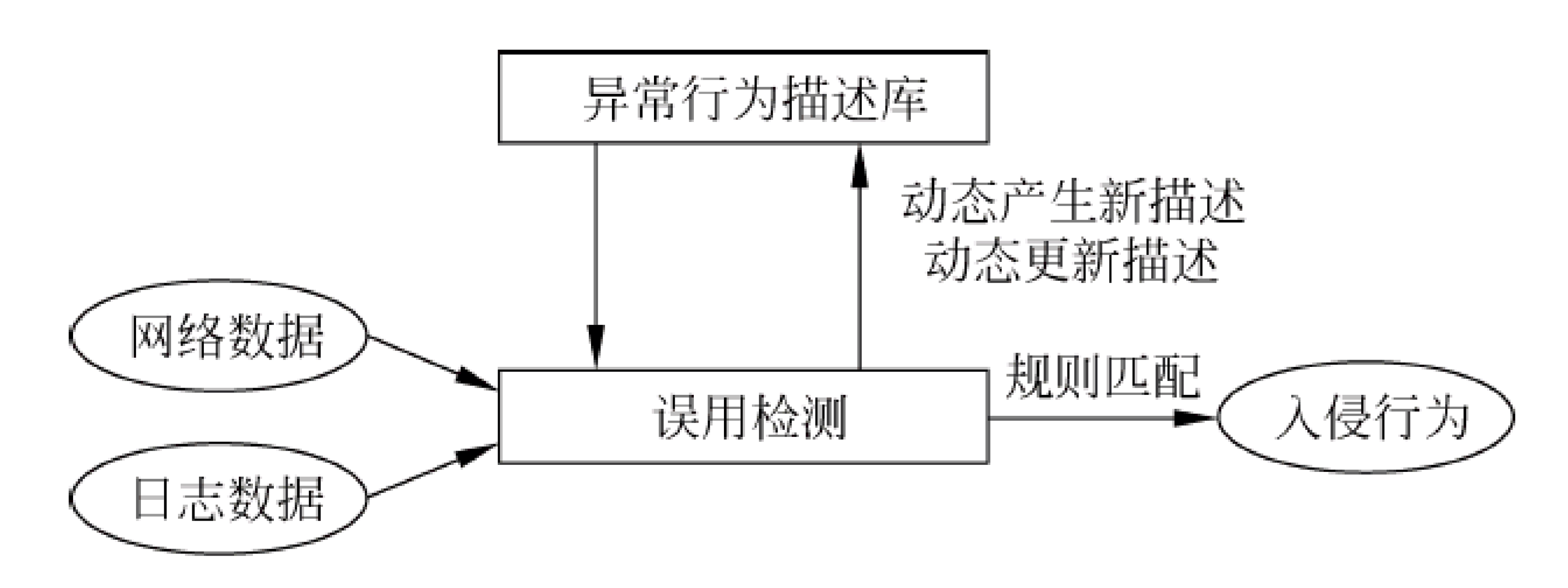


图 7-5 误用检测模型的结构

误用检测技术的优点在于可以准确地检测已知的入侵行为，缺点是不能检测未知的入侵行为。

2. 误用检测基本方法

误用检测是一个“总结入侵特征，确定攻击”的过程，它的主要特点体现在特征库的建立。其主要的检测方法有专家系统、模型推理等。

1）基于专家系统的检测

安全检测工作的另外一个值得重视的研究方向是基于专家系统的攻击检测技术，即根

据安全专家对可疑行为的分析经验来形成一套推理规则，然后再在此基础上建立相应的专家系统。专家系统对所涉及的攻击操作自动进行分析工作。

所谓专家系统，是基于一套由专家经验事先定义的规则的推理系统。例如，某个用户在数分钟之内连续进行登录，且失败次数超过三次，专家系统就可以认为这是一种攻击行为。类似的规则在统计系统中似乎也有，但要注意的是基于规则的专家系统或推理系统也有其局限性，因此作为这类系统的基础推理规则一般都是根据已知的安全漏洞进行安排和策划的，而对系统的最危险的威胁则主要来自未知的安全漏洞。实现基于规则的专家系统是一个知识工程问题，而且其功能应当能够随着经验的积累而利用其自学能力进行规则的扩充和修正。当然，这种能力需要在专家的指导和参与下才能实现，否则可能会导致较多的错误。一方面，推理机制使得系统面对一些新的行为现象时可能具备一定的应对能力（即有可能发现一些新的安全漏洞）；另一方面，攻击行为也可能不会触发任何一个规则，从而还被检测到。总的来说，专家系统对历史数据的依赖性比基于统计技术的审计系统少，因此系统的适应性比较强，可以较灵活地适应广泛的安全策略和检测需求。但迄今为止，推理系统和谓词演算的可计算问题还未得到很好的解决。

在具体实现过程中，专家系统主要面临的问题如下。

（1）全面性问题：很难从各种入侵检测手段中抽象出全面的规则化知识。

（2）效率问题：需要处理的数据量过大，而且在大型系统上很难获得实时、连续的审计数据。

2）基于模型推理的检测

攻击者在攻击一个系统时往往采用一定的行为程序，如猜测口令的程序，这种行为程序构成了某种具有一定行为特征的模型，根据这种模型所代表的攻击意图的行为特征，可以实时地检测出恶意的攻击企图。用基于模型的推理方法，人们能够为某些行为建立特定的模型，从而能够监视具有特定行为特征的某些活动。根据假设的攻击脚本，这种系统就能够检测出非法的用户行为。为了准确判断，一般要为不同的攻击者和不同的系统建立不同的攻击脚本。

当有证据表明某种特定的攻击发生时，系统应收集其他证据来证实或否定攻击的真实性，既不能漏报攻击对信息系统造成实际损害，又能尽量避免错报。

当然，上述几种方法都不能彻底解决攻击检测问题，所以最好是综合地利用各种手段强化计算机信息系统的安全程序，以增加攻击成功的难度，同时根据系统本身的特点选择适合的攻击检测手段。

7.5 入侵检测的特点与发展趋势

7.5.1 入侵检测系统的优点和局限性

入侵检测系统是企业安全防御系统中的重要部件，但入侵检测系统并不是万能的。入侵检测系统对于部分事件可以处理得很好，但对于另一些情况则无能为力。只有充分了解入侵检测系统的优点和局限性，才能对入侵检测系统有一个准确的定位，以便将入侵检测系统有效地应用在安全防御系统中，最大程度地发挥它的安全防御功能。

1. 入侵检测系统的优点

入侵检测系统作为一个迅速崛起并受到广泛认可的安全组件,有着很多方面的安全优势:

(1) 可以检测和分析系统事件以及用户的行为;

(2) 可以检测系统设置的安全状态;

(3) 以系统的安全状态为基础,跟踪任何对系统安全的修改操作;

(4) 通过模式识别等技术从通信行为中检测出已知的攻击行为;

(5) 可以对网络通信行为进行统计,并进行检测分析;

(6) 管理操作系统认证和日志机制并对产生的数据进行分析处理;

(7) 在检测到攻击的时候,通过适当的方式进行适当的报警处理;

(8) 通过对分析引擎的配置对网络的安全进行评估和监督;

(9) 允许非安全领域的管理人员对重要的安全事件进行有效的处理。

2. 入侵检测系统的局限性

入侵检测系统只能对网络行为进行安全审计,从入侵检测系统的定位可以看出,入侵检测系统存在以下缺陷。

(1) 入侵检测系统无法弥补安全防御系统中的安全缺陷和漏洞。这些安全缺陷和漏洞包括其他安全设备的错误配置造成的安全漏洞,以及安全设备本身的实现造成的安全缺陷。入侵检测系统可以通过审计报警对这些可能的安全漏洞进行揭示和定位,但却不能主动对这些漏洞进行弥补,而这些报警信息只有通过人为的补救处理才具有意义。

(2) 对于高负载的网络或主机,很难实现对网络入侵的实时检测、报警和迅速地进行攻击响应。同时,对于高负载的环境,如果没有采用代价较大的负载均衡措施,入侵检测系统会存在较大的分析遗漏,容易造成较大的漏报警率。

(3) 基于知识的入侵检测系统很难检测到未知的攻击行为。即检测具有一定的滞后性,而对于已知的报警,一些没有明显特征的攻击行为也很难检测到,或需要付出提高误报警率的代价才能够正确检测。而基于行为特征的入侵检测系统只能在一定程度上检测到新的攻击行为,但一般很难给新的攻击定性,提供给系统管理员的处理信息较少,很难进行进一步的防护处理。

(4) 入侵检测系统的主动防御功能和联动防御功能会对网络的行为产生影响,同样也会成为攻击者的目标,实现以入侵检测系统自动防御为基础的攻击。通过发送伪造的数据,触发入侵检测系统的主动防御响应,对可信连接进行阻断,造成拒绝服务攻击。在目前的技术条件下,对于网络的主动防御的设置应十分慎重,防止出现利用主动防御系统进行网络攻击的情况。

(5) 入侵检测系统无法单独防止攻击行为的渗透,只能调整相关网络设备的参数或人为地进行处理。由于入侵检测技术不可避免地存在着大量的误报情况,因此进行自动防御会造成对可信连接的影响。目前的入侵检测系统在实质性安全防御方面,还是要以人为修正为主,即使是对可确定入侵的自动阻断行为,建议也要经过人为干预,防止可能的过度防御。

(6) 网络入侵检测系统在纯交换环境下无法正常工作,只有对交换环境进行一定的处理,利用镜像等技术,网络入侵检测系统才能对镜像的数据进行分析处理。因此,在交换环境中,进行各个方向的检测分析将非常困难并且代价较大。

(7) 入侵检测系统主要是对网络行为进行分析检测,不能修正信息资源中存在的安全问题。

7.5.2 入侵检测技术的发展趋势

1. 分析技术的改进

入侵检测误报和漏报的解决最终依靠分析技术的改进。目前入侵检测分析方法主要有统计分析、模式匹配、完整性分析等。

2. 内容恢复和网络审计功能的引入

入侵检测的最高境界是行为分析，但行为分析目前还不是很成熟，因此个别优秀的入侵检测产品引入了内容恢复和网络审计功能。

内容恢复即在协议分析的基础上，对网络中发生的行为加以完整的重组和记录，网络中发生的任何行为都逃不过它的监视。网络审计即对网络中所有的连接事件进行记录。入侵检测的接入方式决定入侵检测系统中的网络审计不仅类似防火墙可以记录网络进出信息，还可以记录网络内部连接状况，此功能对内容恢复无法恢复的加密连接尤其有用。

内容恢复和网络审计让管理员看到网络的真正运行状况，其实就是调动管理员参与行为分析过程。此功能不仅能使管理员看到孤立的攻击事件的报警，还可以看到整个攻击过程，了解攻击确实发生与否，查看攻击者的操作过程，了解攻击造成的危害；不但能发现已知攻击，还能发现未知攻击；不但发现外部攻击者的攻击，也能发现内部用户的恶意行为。管理员是最了解其网络的，管理员通过此功能的使用，很好地达到了行为分析的目的。但使用此功能的同时需注意对用户隐私的保护。

3. 集成网络分析和管理功能

入侵检测不但对网络攻击是一个检测，还可以收到网络中的所有数据，对网络的故障分析和健康管理也可起到重大作用。当管理员发现某台主机有问题时，也希望能马上对其进行管理。入侵检测不应只采用被动的分析方法，最好能和主动分析结合。所以，入侵检测产品以后发展的方向是集成网管、扫描器、嗅探器等功能。

4. 安全性和易用性的提高

入侵检测是个安全防护产品，自身安全极为重要。因此，目前的入侵检测产品大多采用硬件结构，黑洞式接入，以免除自身安全问题。同时，入侵检测产品对易用性的要求也日益增强，如全中文的图形界面、自动的数据库维护、多样的报表输出。这些都是优秀入侵检测产品的特性和以后继续发展细化的趋势。

5. 改进对大数据量网络的处理方法

随着对大数据量处理的要求，入侵检测的性能要求也逐步提高，出现了千兆入侵检测等产品。但如果入侵检测产品不仅具备攻击分析功能，同时具备内容恢复和网络审计功能，则其存储系统一般工作在千兆环境以上。这种情况下，网络数据分流也是一个很好的解决方案，性价比较高，这也是国际上较通用的一种做法。

6. 防火墙联动功能

入侵检测发现攻击，自动发送给防火墙，防火墙加载动态规则拦截入侵，称为防火墙联动功能。目前此功能还没有到完全实用的阶段，主要是一种概念，随便使用会导致很多问题。目前该功能主要的应用对象是自动传播的攻击，如 Nimda 等，联动只在这种场合有一定的作用。无限制地使用联动，如未经充分测试，对防火墙的稳定性和网络应用会造成负面影响。但随着入侵检测产品检测准确度的提高，联动功能日益趋向实用化。

7.6 入侵检测系统示例

为了直观地理解入侵检测的使用、配置等情况，下面以 Snort 为例对构建以 Snort 为基础的入侵检测系统进行介绍。

Snort 是开源、高度可配置且可移植的基于主机或基于网络的 IDS。Snort 被称为是轻量级 IDS，它具有以下特征：

(1) 可以在大多数网络节点(主机、服务器和路由器)轻松地部署。

(2) 使用少量的内存和处理时间进行高效操作。

(3) 系统管理员可以容易地进行配置，以便在较短时间内实现特定的安全解决方案。

Snort 可以进行实时数据包的捕获、协议分析以及内容搜索与匹配。根据一组由系统管理员配置的规则，Snort 能够检测到很多种攻击和探测。

7.6.1 Snort 体系结构

一个 Snort 包括以下 4 个逻辑组件，如图 7-6 所示。

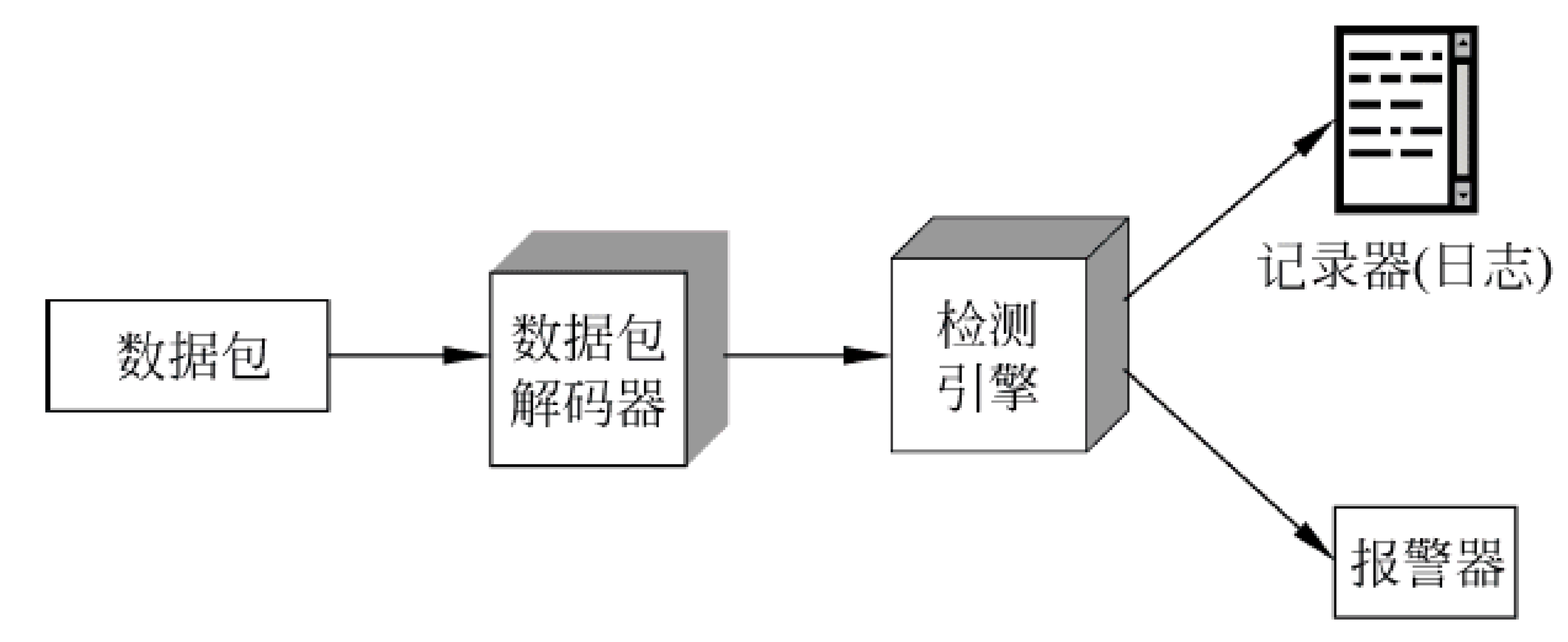


图 7-6 Snort 体系结构

(1) 数据包解码器(packet decoder)：数据包解码器处理每个捕获的数据包，在数据链路层、网络层、传输层和应用层识别并分离协议首部。解码器被设计为尽可能地高效，它的主要工作包括设置指针，以便可以很容易地提取各种协议首部。

(2) 检测引擎(detection engine)：检测引擎完成入侵检测的实际工作。本模块基于一组由安全管理员配置的 Snort 规则来分析每个数据。从本质上讲，每个数据包依据所有规则进行检查，以确定该数据包是否与根据规则定义的特征相匹配，与已解码的数据包匹配的第一个规则触发规则指定的动作，如果没有规则匹配该数据包，则检测引擎放弃此数据包。

(3) 记录器(logger)：对于每个与规则匹配的数据包，该规则指定什么日志和报警选项是要执行的。当选定一个记录器选项时，记录器存储检测到的数据包以可读格式或更加紧凑的二进制格式存储在指定的日志文件中，然后安全管理员可以使用日志文件进行以后的分析。

(4) 报警器(alerter)：对于每个检测到的数据包，发送一个警报。匹配规则中的报警选项确定事件通知中包括哪些信息。事件通知可以发送到文件、UNIX 套接字或者数据库。警报也可以在测试或渗透研究期间关闭，使用 UNIX 套接字，可以将通知发送到网络上其他地方的管理机。

7.6.2 Snort 规则

Snort 使用一种简单、灵活的规则来定义生成检测引擎使用的规则的语言。尽管规则

非常简单，可以直接编写，但它们的功能可以检测各种恶意或可疑的网络流量。Snort 规则格式如图 7-7 所示。

动作	协议	源IP地址	源端口	方向	目的IP地址	目的端口
选项关键字	选项参数	…				

图 7-7　Snort 规则格式

每个规则包括一个固定的首部和 0 个或多个选项，首部包含以下元素。

（1）动作（action）：规则动作告诉 Snort 当它找到符合规则条件的数据包时应如何去做。表 7-1 列出了可用的动作。列表中的最后三个动作只在内嵌模式下可用。

表 7-1　Snort 规则动作

动　作	说　明
alert	使用所选的报警方式生成警报，再将数据包写入日志
log	将数据包写入日志
pass	忽略数据包
activate	报警后再激活另一个 dynamic 规则
dynamic	保持空闲直到被 activate 规则激活，然后作为 log 规则
drop	使 iptables 丢弃数据包并写入日志
reject	使 iptables 丢弃数据包，记入日志，并发送数据，如果协议是 TCP，发送 TCP 重置；如果协议是 UDP，则发送 ICMP 端口不可达消息
sdrop	使 iptables 丢弃数据包但不写入日志

（2）协议（prococol）：Snort 继续分析数据包协议是否匹配这个字段。Snort 的目前版本支持 4 个协议，包括 TCP、UDP、ICMP 和 IP。Snort 的未来版本将支持更多的协议。

（3）源 IP 地址（source IP address）：指明数据包的源。该规则可以指定特定的 IP 地址、任何 IP 地址和特定的 IP 地址列表，或者拒绝特定的 IP 地址或 IP 地址列表。拒绝表示在列表之外的任何 IP 地址都是匹配的。

（4）源端口（source port）：该字段指出用于指定协议的源端口（如 TCP 端口）可以以多种方式指定端口号，包括特定端口号、任何端口、静态端口定义、端口范围和拒绝某些端口。

（5）方向（direction）：该字段采用单向或双向选项，双向选项告诉 Snort 应该将规则中的地址/端口对理解为前面是源后面是目的，或者前面是目的后面是源。利用双向选项，Snort 能够监控对话的双方。

（6）目的 IP 地址（destination IP address）：指明数据包的目的地址。

（7）目的端口（destination port）：指明目的端口。

在规则首部之后可以有一个或多个规则选项。每个选项由选项关键字组成，关键字定义选项；后面跟着参数，指定选项的详细信息。在书面形式中，规则选项集被括在括号中与首部分开。Snort 规则选项用分号分隔，规则选项关键字与其参数用冒号分隔。

Snort 有以下 4 个主要类别的规则选项。

（1）元数据（meta-data）：提供关于规则的信息，但在检测期间不起任何作用。

（2）有效载荷（payload）：查找有效载荷数据包中的数据，可以是相关的。

（3）非有效载荷（non-payload）：查找非有效载荷数据。

(4) 后检测(post-detection):当规则匹配一个数据包后引发的特定规则。

7.6.3 Snort 的安装与使用

1. Snort 的安装模式

Snort 可安装为守护进程模式,也可安装为包括很多其他工具的完整的入侵检测系统。简单方式安装 Snort 时,可以得到入侵数据的文本文件或二进制文件,然后用文本编辑器等工具进行查看。在这种安装模式下,Snort 可将警报信息以 SNMP trap 的形式发送到类似于 HP OpenView 或 OpenNMS 之类的网管系统上,也可以 SMP 弹出窗口的形式发送到运行 Windows 操作系统的计算机上。

Snort 若与其他工具一起安装,则可以支持更为复杂的操作。例如,将 Snort 数据发送给数据库系统,从而支持通过 Web 界面进行数据分析,以增强对 Snort 捕获数据的直观认识,避免耗费大量时间查阅日志文件。

2. Snort 的简单安装

Snort 的安装程序包括 Linux 平台程序和 Windows 平台程序,所有安装程序可以在 Snort 官方网站上获取。Linux 平台下通常使用源代码包的形式进行安装,可以方便进行参数配置,下面介绍 Linux 平台下 Snort 源代码包的简单安装方法。

1) 安装 Snort

Snort 的正常运行必须要有 libpcap 库的支持,因此在安装 Snort 之前需要确认系统已经安装了 libpcap 库,若未安装,可以到官方网站下载。

```
[root@ mail snort-2.8.0]# ./configure - - enable-dynamicplugin
[root@ mail snort-2.8.0]# make
[root@ mail snort-2.8.0]# make install
```

其中,--enable-dynamicplugin 是为了产生/usr/local/lib/snort_dynamicpreprocessor/这个目录,否则启动 snort 为 Network Intrusion Detection System Mode 模式时会出现如下错误:

```
FATAL ERROR: /etc/snort/snort.conf(183) = > Unknown rule type: dynamicpreprocessor
```

更多安装选项请参阅 doc/INSTALL 文件。

2) 更新 Snort 规则

下载最新的规则文件 snortrules-snapshot-CURRENT.tar.gz。其中,CURRENT 表示最新的版本号。

```
[root@ mail snort]# mkdir /etc/snort
[root@ mail snort]# cd /etc/snort
[root@ mail snort]# tar zxvf /path/to/snortrules-snapshot-CURRENT.tar.gz
```

3) 配置 Snort

建立 config 文件目录:

```
[root@ mail snort-2.8.0]# mkdir/etc/snort
```

复制 Snort 配置文件 snort.conf 到 Snort 配置目录:

```
[root@ mail snort-2.8.0]# cp./etc/snort.conf/etc/snort/
```

编辑 snort.conf：

```
[root@ mail snort-2.8.0]# vi/etc/snort/snort.conf
```

修改后，一些关键设置如下：

```
var HOME_NET yournetwork
var RULE_PATH /etc/snort/rules
preprocessor http_inspect: global
iis_unicode_map /etc/snort/rules/unicode.map 1252
include /etc/snort/rules/reference.config
include /etc/snort/rules/classification.config
```

4）测试 Snort

```
# /usr/local/bin/snort -A fast -b -d -D -l /var/log/snort -c /etc/snort/snort.conf
```

查看文件/var/log/messages，若没有错误信息，则表示安装成功。

5）将日志写入 mysql 数据库

建立数据库：

```
% echo "CREATE DATABASE snort;" | mysql -u root -p
```

建立表（使用 schemas/create_mysql 文件）：

```
% mysql -D snort -u root -p < ./schemas/create_mysql
```

建立用户及权限：

```
mysql > set password for 'snortusr '@'localhost' = password('mypassword')
```

修改 snort.conf 文件：

```
output database: log,mysql,user = snortusr password = mypassword dbname = snort host = localhost
```

3. Snort 的工作模式

Snort 有三种工作模式，即嗅探器、数据包记录器及网络入侵检测系统。嗅探器模式仅从网络上读取数据包并不断地显示在终端上；数据包记录器模式则把数据包记录到硬盘上；网络入侵检测模式最为复杂，而且可配置。

1）嗅探器

所谓的嗅探器模式就是 Snort 从网络上获取数据包然后显示在控制台上。若只把 TCP/IP 包头信息打印在屏幕上，则只需要执行下列命令：

```
./snort -v
```

若显示应用层数据，则执行：

```
./snort -vd
```

若同时显示数据链路层信息，则执行：

```
./snort -vde
```

2）数据包记录器

如果要把所有的数据包记录到硬盘上，则需要指定一个日志目录，Snort 将会自动记录数据包：

```
./snort -dev -l ./log
```

当然，./log 目录必须存在，否则 Snort 就会报告错误信息并退出。当 Snort 在这种模式下运行时，它会记录所有捕获的数据包，并将其放到一个目录中，该目录以数据包目的主机的 IP 地址命名，如 192.168.8.112。

如果网络速度很快，或者希望日志更加紧凑以便事后分析，则应该使用二进制日志文件格式。使用下面的命令可以把所有的数据包记录到一个单一的二进制文件中：

```
./snort -l ./log -b
```

随后可以使用任何支持 tcpdump 二进制格式的嗅探器程序从该文件中读出数据包，如 tcpdump 或者 Ethereal。使用 -r 功能开关，也可使 Snort 读出包中的数据。Snort 在所有运行模式下都能够处理 tcpdump 格式的文件。

对于希望在嗅探器模式下把一个 tcpdump 格式的二进制文件内容显示到屏幕上，可以输入下面的命令：

```
./snort -dv -r packet.log
```

在数据包和入侵检测模式下，通过 BPF 接口可以使用多种方式维护日志文件中的数据。例如，希望从日志文件中提取 ICMP 包，只需要输入下面的命令行：

```
./snort -dvr packet.log icmp
```

3）网络入侵检测系统

通过下面命令行，可以将 Snort 启动为网络入侵检测系统模式：

```
./snort -dev -l ./log -h 192.168.8.0/24 -c snort.conf
```

snort.conf 是规则集文件。Snort 会将每个包和规则集进行匹配，一旦匹配成功就会采取响应措施。若不指定输出目录，Snort 就将日志输出到/var/log/snort 目录。

在网络入侵检测模式下，可以有多种方式配置 Snort 的输出。在默认情况下，Snort 以 ASCII 格式记录日志，使用 full 报警机制。如果使用 full 报警机制，Snort 会在包头之后打印报警消息。如果不需要日志包，可以使用 -N 选项进行关闭。

Snort 有六种报警机制：full、fast、socket、syslog、smb 和 none。其中下列 4 个机制可以在命令状态下使用 -A 选项进行设置。

（1）-A fast：报警信息包括时间戳、报警消息、源/目的 IP 地址和端口。

（2）-A full：默认报警模式。

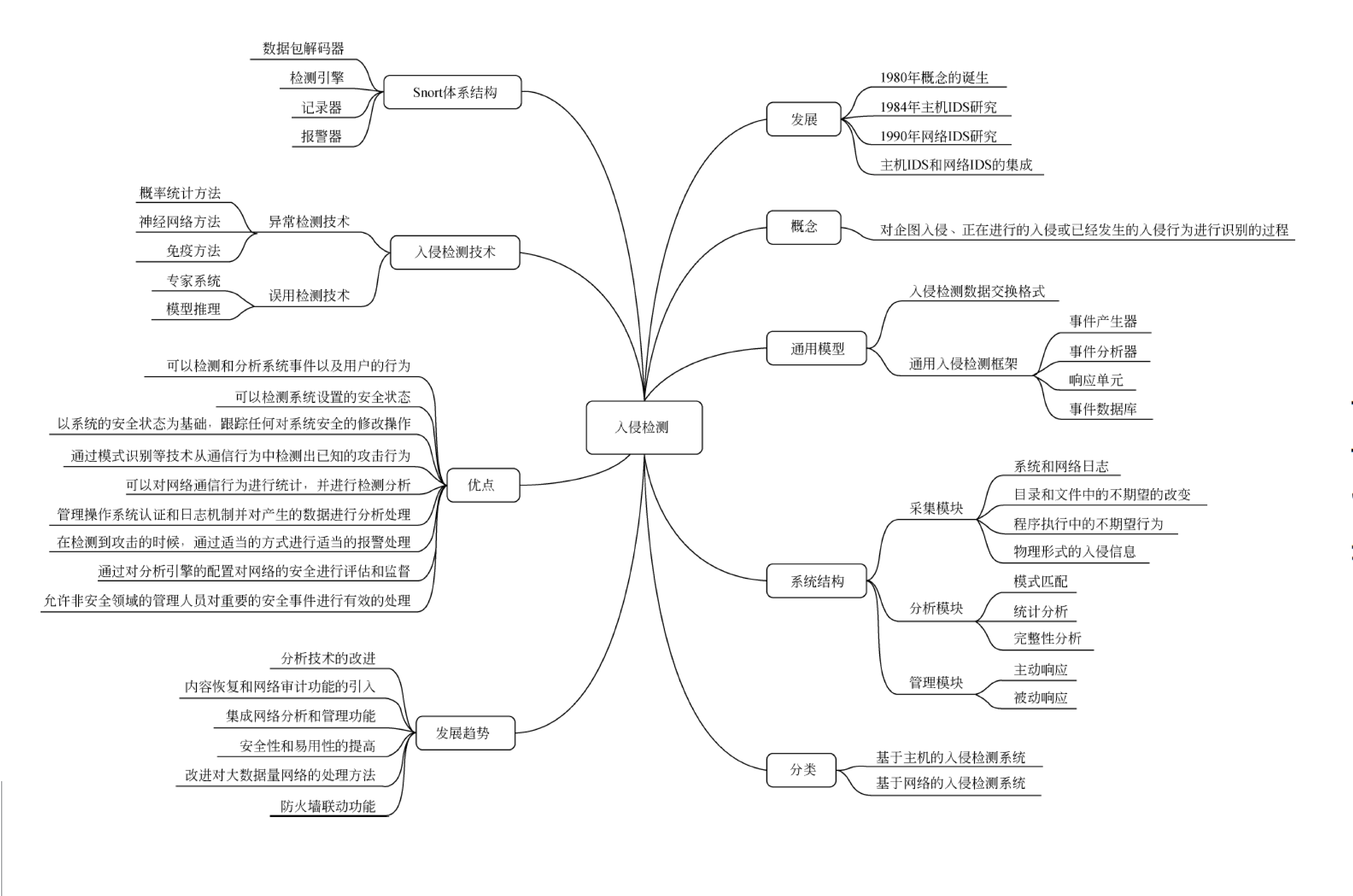
（3）-A socket：把报警信息发送到一个 UNIX 套接字。

（4）-A none：关闭报警机制。

使用 -s 选项可以使 Snort 把报警消息发送到 syslog，默认的设备是 LOG_AUTHPRIV 和 LOG_ALERT。可以修改 snort.conf 文件更改其配置。

Snort 还可以使用 SMB 报警机制，通过 SAMBA 把报警消息发送到 Windows 主机。为了使用这个报警机制，在运行./configure 脚本时，必须使用--enable-smbalerts 选项。

7.7 本章小结



入侵检测
发展
1980年概念的诞生
1984年主机IDS研究
1990年网络IDS研究
主机IDS和网络IDS的集成
概念
对企图入侵、正在进行的入侵或已经发生的入侵行为进行识别的过程
通用模型
入侵检测数据交换格式
通用入侵检测框架
事件产生器
事件分析器
响应单元
事件数据库
系统结构
采集模块
系统和网络日志
目录和文件中的不期望的改变
程序执行中的不期望行为
物理形式的入侵信息
分析模块
模式匹配
统计分析
完整性分析
管理模块
主动响应
被动响应
分类
基于主机的入侵检测系统
基于网络的入侵检测系统
Snort体系结构
数据包解码器
检测引擎
记录器
报警器
入侵检测技术
异常检测技术
概率统计方法
神经网络方法
免疫方法
误用检测技术
专家系统
模型推理
优点
可以检测和分析系统事件以及用户的行为
可以检测系统设置的安全状态
以系统的安全状态为基础，跟踪任何对系统安全的修改操作
通过模式识别等技术从通信行为中检测出已知的攻击行为
可以对网络通信行为进行统计，并进行检测分析
管理操作系统认证和日志机制并对产生的数据进行分析处理
在检测到攻击的时候，通过适当的方式进行适当的报警处理
通过对分析引擎的配置对网络的安全进行评估和监督
允许非安全领域的管理人员对重要的安全事件进行有效的处理
发展趋势
分析技术的改进
内容恢复和网络审计功能的引入
集成网络分析和管理功能
安全性和易用性的提高
改进对大数据量网络的处理方法
防火墙联动功能

7.8 习　　题

一、填空题

1. CIDF 模型将入侵检测系统分为事件产生器、(　　)、响应单元和事件数据库 4 个组件。

2. 入侵检测系统一般包括(　　)、分析模块和管理模块三个部分。

3. 入侵检测系统分析模块一般通过(　　)、统计分析和完整性分析三种技术进行分析。

4. (　　)又称为基于行为的入侵检测技术，用来识别主机或网络的异常行为。

5. (　　)的检测技术的基本思想是用一系列信息单元训练神经单元，在给定一个输入后，就可能预测出输出。

二、选择题

1. 以下不是产生入侵检测系统的原因的是(　　)。
   A. 与攻击有关的信息流无处不在
   B. 攻击行为与正常访问过程存在差距
   C. 杀毒软件不具有发现非法资源访问操作的功能
   D. 控制网络间数据交换过程

2. 关于入侵检测系统，以下描述错误的是(　　)。
   A. 一般的入侵检测系统和杀毒软件一样，需要定时更新攻击特征库
   B. 正常访问过程和入侵过程存在差异，但无法严格区分
   C. 规则是长期观察信息流变化过程后得出的一些规律性的总结
   D. 入侵检测系统能够检测出没有发作的病毒

3. 以下关于入侵检测系统功能的描述错误的是(　　)。
   A. 防御病毒发作引发的攻击行为　　B. 防御对资源的非法访问
   C. 防御分布式拒绝服务攻击　　D. 防御信息嗅探和截获攻击

4. 入侵检测系统能够防御的攻击行为是(　　)。
   A. 路由项欺骗攻击　　B. 重放攻击
   C. DNS 欺骗攻击　　D. 源 IP 地址欺骗攻击

5. 入侵检测的目的是(　　)。
   A. 实现内外网隔离与访问控制
   B. 提供实时的检测及采取相应的防护手段
   C. 记录用户使用计算机网络系统进行所有活动的过程
   D. 预防、检测和消除病毒

6. 关于入侵检测系统功能，以下描述错误的是(　　)。
   A. 捕获流经关键链路的信息流　　B. 发现攻击行为
   C. 反制攻击行为　　D. 预防攻击行为

7. 不是入侵检测系统通用框架中的构件的是(　　)。
   A. 事件发生器　　B. 事件分析器　　C. 事件数据库　　D. 事件捕获器

8. 关于基于主机的入侵检测系统，以下描述错误的是(　　)。

A. 利用攻击特征库发现攻击行为

B. 根据访问授权发现非法资源访问过程

C. 禁止非法 TCP 连接建立

D. 保证主机不感染病毒

9. 异常检测 IDS 使用(　　)方法进行分析。

A. 模式匹配　　B. 统计分析　　C. 完整性分析　　D. 可用性分析

10. 误用检测 IDS 的特点是(　　)。

A. 误报低、漏报高　　B. 误报高、漏报低

C. 误报低、漏报低　　D. 误报高、漏报高

三、判断题

1. 入侵检测系统是一种积极主动的安全防护技术。

2. 入侵检测系统的采集模块主要用来信息收集，收集的内容包括系统、网络、数据及用户活动的状态和行为。

3. 模式匹配就是将收集到的信息与已知的网络入侵和系统误用模式数据库进行比较，从而发现违背安全策略的行为。

4. 基于网络的入侵检测系统具有可以确定攻击是否成功的优点。

5. 基于网络的入侵检测系统只能检查它直接连接网段的通信，不能检测在不同网段的数据包。

6. 异常检测是一个“学习正常，发现异常”的过程，它的主要特点体现在学习过程中。

7. 基于概率统计的检测技术是异常入侵检测中最常用的技术，它对用户历史行为建立模型。

8. 误用检测是一个“总结入侵特征，确定攻击”的过程，它的主要特点体现在特征库的建立。

9. 入侵检测系统可以弥补安全防御系统中的安全缺陷和漏洞。

10. Snort 是开源、高度可配置且可移植的基于主机或基于网络的 IDS。

四、简答题

1. 根据入侵检测系统的检测对象的不同，入侵检测系统主要分为哪两类？这两类入侵检测系统的数据源分别是什么？

2. 基于主机的入侵检测系统的优点是什么？

第8章 密　码　学

【本章学习目标】

- 了解密码系统的组成
- 了解密码体制分类
- 理解对称加密体制与非对称加密体制
- 掌握 DES 和 RSA 加密技术
- 了解信息加密体制应用

8.1 密码学概述

8.1.1 密码学基本概念

密码学是研究如何实现秘密通信的科学，它包括两个分支，即密码编码学和密码分析学。

密码编码学是关于消息保密的技术和科学。密码编码学是密码体制的设计学，即怎样编码，采用什么样的密码体制保证信息被安全地加密。从事此行业的人员被称为密码编码者。

密码分析学是与密码编码学相对应的技术和科学，即研究如何破译密文的科学和技术。密码分析学是在未知密钥的情况下从密文推出明文或密钥的技术。密码分析者是从事密码分析的专业人员。

8.1.2 现代密码系统的组成

现代密码系统（一般简称为密码体制）一般由以下 5 个部分组成。

(1) 明文空间 M：它是全体明文的集合，记为 $M=[M_1, M_2, \cdots, M_n]$。明文用 M(消息)或 P(明文)表示，它一般是比特流，明文可被传送或存储，无论在哪种情况下，M 均指待加密的消息。

(2) 密文空间 C：它是全体密文的集合，记为 $C=[C_1, C_2, \cdots, C_n]$。明文加密后的形式为密文。

(3) 密钥空间 K：它是全体密钥的集合。加密和解密操作在密钥的控制下进行。密钥空间 K 通常由加密密钥和解密密钥组成，即 $K=(K_e, K_d)$。

(4) 加密算法 E：它是一族由 M 到 C 的加密变换，对于每一个具体的 K_e，E 确定出一个具体的加密函数，把 M 加密成密文 C，通常记为 $C=E(M, K_e)$ 或 $C=E_{K_e}(M)$。

(5) 解密算法 D：它是一族由 C 到 M 的解密变换，对于每一个确定的 K_d，D 确定出一个具体的解密函数，把密文 C 恢复为 M，通常记为 $M=D(C, K_d)$ 或 $M= D_{K_d}(C)$。

一个有意义的密码系统应当满足的条件为：对于每一确定的密钥 $K=(K_e,K_d)$，有 $M=D(C,K_d)=D(E(M,K_e),K_d)$，或记为 $M=D_{Kd}(E_{Ke}(M))$。一般地，密码系统的模型可用图 8-1 表示。

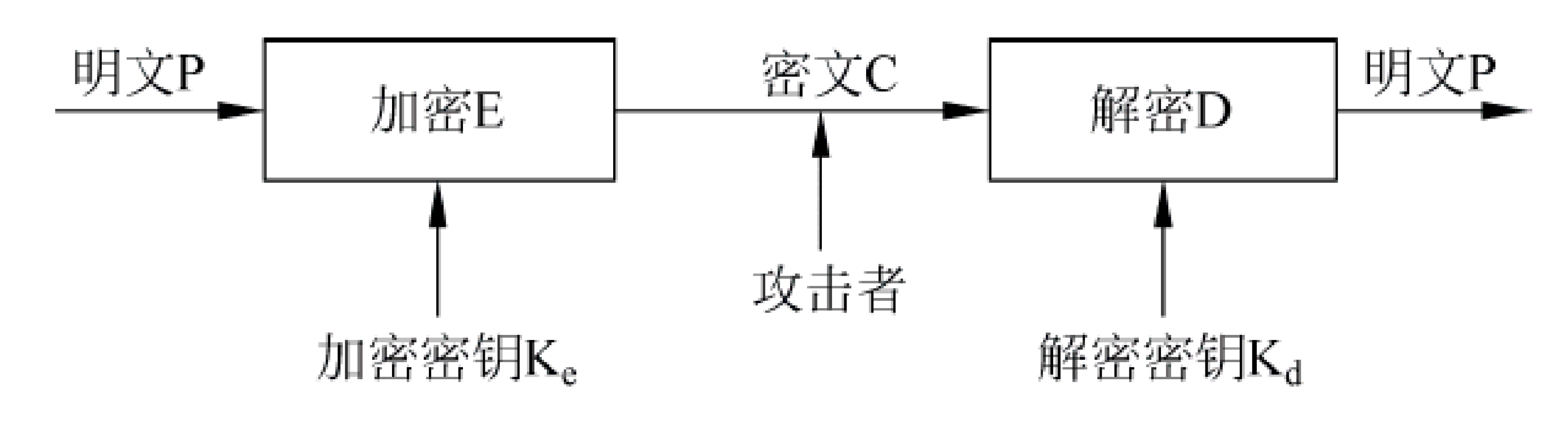


图 8-1　一般密码系统示意图

8.1.3　密码算法的安全性

根据被破译的难易程度，不同的密码算法具有不同的安全等级。如果破译算法的代价大于加密数据的价值，那么算法可能是安全的；如果破译算法所需的时间比加密数据的时间更长，那么算法可能是安全的；如果用单密钥加密的数据量比破译算法需要的数据量少得多，那么算法可能是安全的。

这里说"可能"是因为在密码分析中总有新的突破。在另一方面，大多数数据随着时间的推移，其价值会越来越小，这点是很重要的。

Lars Knudsen 把破译算法分为不同的类别，按安全性的递减顺序可分为：

(1) 全部破译。密码分析者找出密钥 K，这样 $D_K(C)=M$。

(2) 全盘推导。密码分析者找到一个代替算法 A，在不知道密钥 K 的情况下，等价于 $D_K(C)=M$。

(3) 实例推导。密码分析者从截获的密文中找出明文。

(4) 信息推导。密码分析者获得一些有关密钥或明文的信息。这些信息可能是密钥的几个比特、有关明文格式的信息等。

8.2　密码体制分类

密码体制从原理上可分为两大类，即单钥(对称密码体制)和双钥(非对称密码体制)。在传统的对称加密系统中，加密用的密钥与解密用的密钥是相同的，密钥在通信中需要严格保密。在非对称加密系统中，加密用的公钥与解密用的私钥是不同的，加密用的公钥可以向大家公开，而解密用的私钥是需要保密的。

8.2.1　对称加密体制

对称加密技术对信息的加密与解密都使用相同的密钥，因此又称为私钥密码技术。使用对称加密方法，加密方与解密方必须使用同一种加密算法和相同的密钥。

图 8-2 给出了对称加密的原理示意图。对称加密体制的基本元素包括原始的明文、加密算法、密钥、密文。

只要通信双方能确保密钥在交换阶段未泄露，那么就可以保证信息的机密性与完整性。对称加密技术存在着通信双方之间确保密钥安全交换的问题。如果一个用户同时与 N 个其

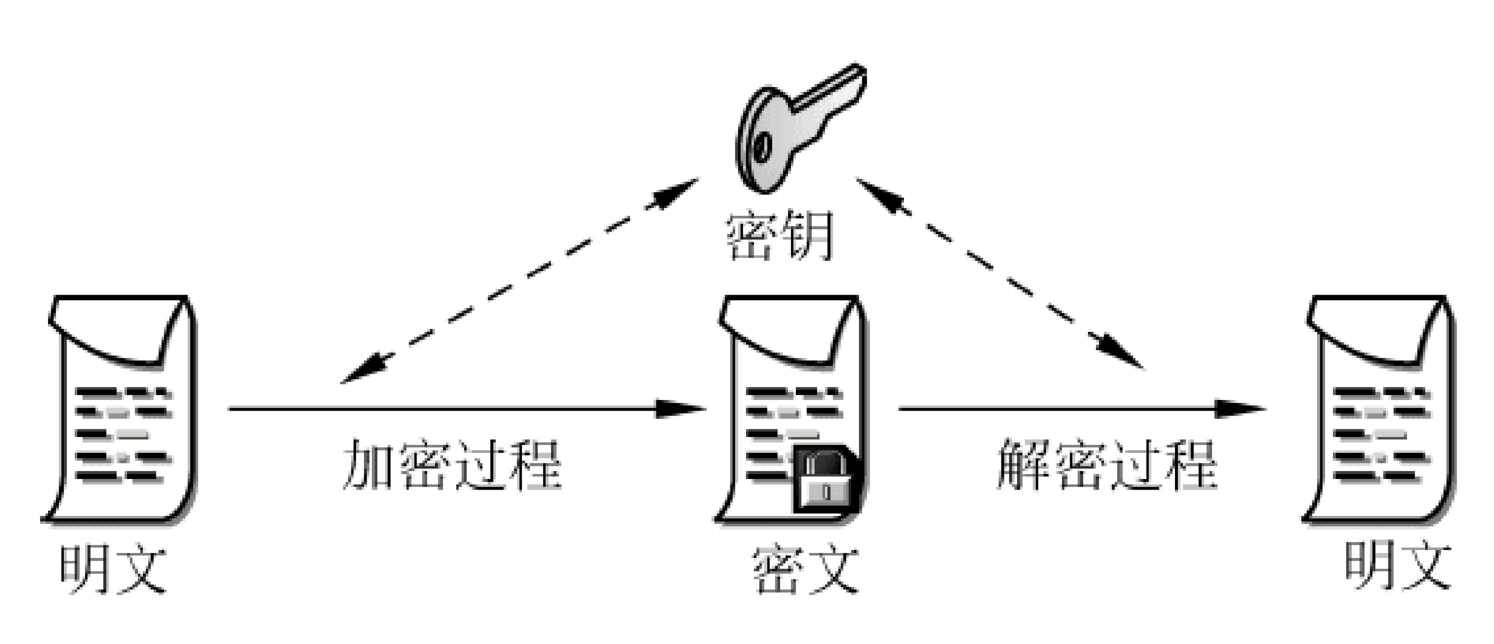


图 8-2 对称加密体制原理示意图

他用户进行通信时,每个用户对应一个密钥,那么他就需要维护 N 个密钥。当网络中有 N 个用户之间进行加密通信时,则需要有 $N(N-1)$个密钥,才能保证任意两方之间的通信。

在对称加密体系中加密方和解密方使用相同的密钥,系统的保密性主要取决于密钥的安全性。因此,密钥在加密方和解密方之间的传递和分发必须通过安全通道进行,在公共网络上使用明文传递密钥是不合适的。如果密钥没有以安全方式传送,那么黑客就很可能非常容易地截获密钥。如何产生满足保密需要的密钥,如何安全、可靠地传送密钥是十分复杂的问题。

对称加密体制的优点主要体现在其加密、解密处理速度快、保密度高等,其缺点主要体现在以下方面。

(1) 密钥是保密通信安全的关键,发信方必须安全、妥善地把密钥护送到收信方,不能泄漏其内容。如何才能把密钥安全地送到收信方,是单钥密码算法的突出问题。单钥密码算法的密钥分发过程十分复杂,所花代价很高。

(2) 多人通信时密钥组合的数量会出现爆炸性膨胀,使密钥分发更加复杂化。n 个人进行两两通信,总共需要的密钥数为 $n(n-1)/2$ 个。

(3) 通信双方必须统一密钥,才能发送保密的信息。如果发信者与收信者素不相识,就无法向对方发送秘密信息了。

(4) 除了密钥管理与分发问题,单钥密码算法还存在数字签名困难的问题。通信双方拥有同样的消息,接收方可以伪造签名,发送方也可以否认发送过某消息。

数据加密标准 DES 是最典型的对称加密算法,它是由 IBM 公司推出,经过国际标准化组织认定的数据加密的国际标准。DES 算法采用了 64 位密钥长度,其中 8 位用于奇偶校验,用户可以使用其余的 56 位。DES 算法并不是非常安全的,入侵者使用运算能力足够强的计算机,对密钥逐个尝试就可以破译密文。但是破译密码需要很长时间,只要破译的时间超过密文的有效期,加密就是有效的。目前已经有一些比 DES 算法更安全的对称加密算法,如 IDEA 算法、RC2 算法、RC4 算法等。

8.2.2 非对称加密体制

非对称加密技术对信息的加密与解密使用不同的密钥,用来加密的密钥是可以公开的公钥,用来解密的密钥是需要保密的私钥,因此又被称为公钥加密技术。

在 1976 年,Diffie 与 Hellman 提出了公钥加密的思想,加密用的公钥与解密用的私钥不同,公开加密密钥不至于危及解密密钥的安全。图 8-3 给出了非对称加密体制的原理示意图。用来加密的公钥(public key)与解密的私钥(private key)是数学相关的,并且加密公钥与解密私钥是成对出现的,但是不能通过加密公钥来计算出解密私钥。

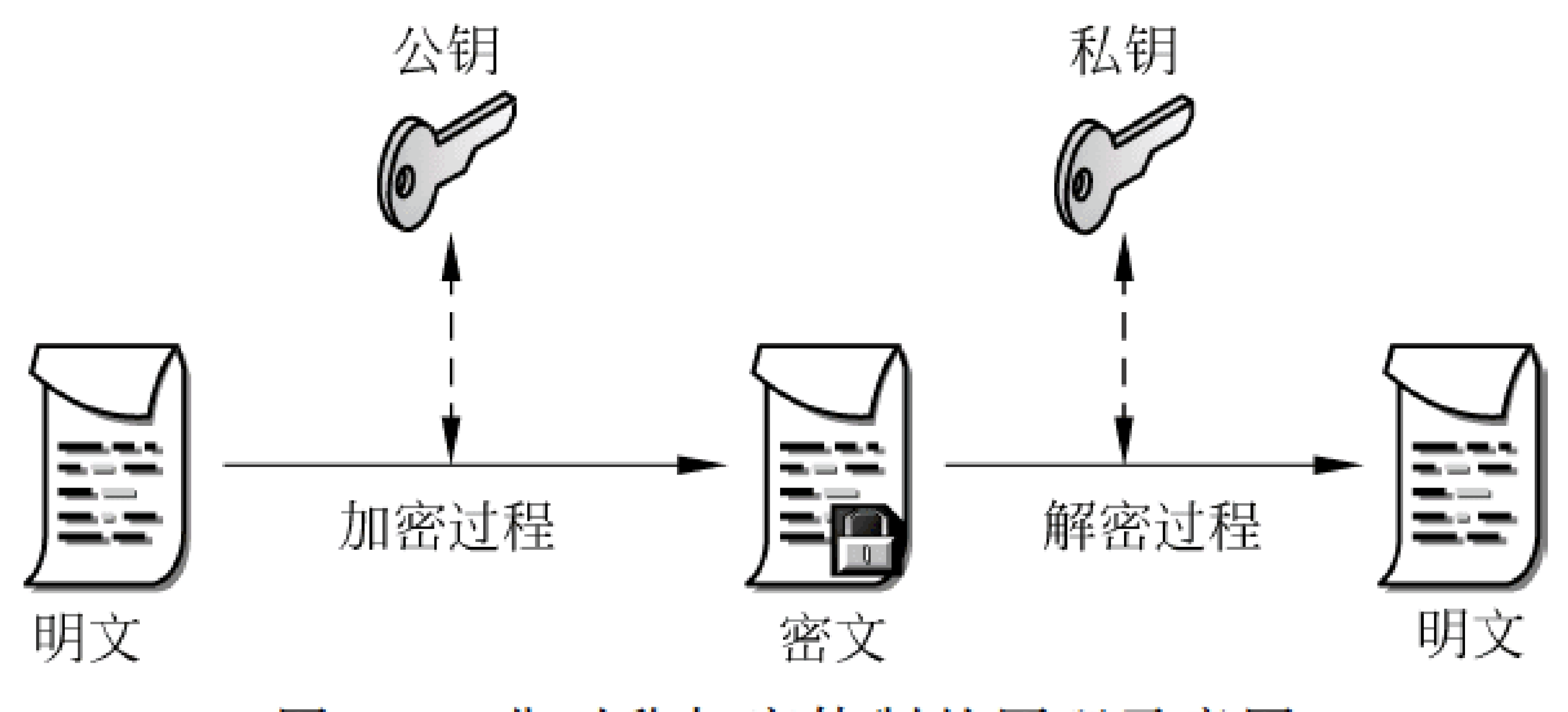


图 8-3　非对称加密体制的原理示意图

非对称密钥密码体制在现代密码学中是非常重要的。按照一般的理解，加密主要是解决信息在传输过程中的保密性问题。但是还存在着另一个问题，那就是如何对信息发送方和接收方的真实身份进行验证，以防止用户对所发出信息和接收信息的事后抵赖，并且能够保证数据完整性。非对称密钥密码体制对这两个方面都给出了很好的解决方案。

在非对称密钥密码体制中，加密的公钥与解密的私钥是不相同的。公钥是公开的，谁都可以使用，而私钥只有解密人自己知道。由于采用了两个密钥，并且从理论上可以保证要从公钥和密文中分析出明文和解密的私钥是不可能的。那么以公钥作为加密密钥，接收方使用私钥解密，就可实现由多个用户发送的密文只能由一个持有解密的私钥的用户解读。相反，如果以用户的私钥作为加密密钥，而以公钥作为解密密钥，则可以实现由一个用户加密的信息由多个用户解读。这样网络中有 N 个用户之间进行加密通信时，不再需要有 $N(N-1)$ 个密钥，并可以用于数字签名。

非对称加密技术可以大大简化密钥的管理。网络中的 N 个用户之间进行通信加密，仅仅需要使用 N 对密钥即可，而且用于解密的私钥不需要发往任何地方，公钥在传递和发布过程中即使被截获，由于没有与公钥相匹配的私钥，截获的公钥对入侵者也就没有太大的意义。这正是非对称加密技术与对称加密技术相比所具有的优势。

公钥加密体制的优点是可以公开加密密钥，适应网络的开放性要求，且仅需保密解密密钥，所以密钥管理问题比较简单。其主要缺点是加密算法复杂，加密与解密的速度比较慢。

RSA 体制是 1978 年由 Rivest、Shamir 和 Adleman 提出的一个公钥密码体制，RSA 就是以其发明者姓名的首字母命名的。RSA 体制被认为是目前为止理论上最为成熟的一种公钥密码体制。RSA 体制多用于数字签名、密钥管理和认证等方面。1985 年，ElGamal 构造了一种基于离散对数的公钥密码，这就是 ElGamal 公钥体制。ElGamal 公钥体制的密文不仅依赖于待加密的明文，而且依赖于用户选择的随机数，由于每一次随机数都是不同的，因此即使加密相同的明文，得到的密文也是不同的。由于这种加密算法的不确定性，又称其为概率加密体制。目前，典型的公钥加密算法还有 Diffie-Hellman 密钥交换、数据签名标准 DSS、椭圆曲线密码等。

8.3　DES 对称加密技术

DES(Data Encryption Standard)算法于 1977 年得到美国政府的正式许可，是一种用 56 位密钥来加密 64 位数据的方法。

8.3.1　DES 算法的原理

DES 算法的入口参数有三个：Key、Data、Mode。其中 Key 为 8 个字节共 64 位，是

DES 算法的工作密钥；Data 也为 8 个字节 64 位，是要被加密或被解密的数据；Mode 为 DES 的工作方式，有加密和解密两种。

DES 算法的原理是：如 Mode 为加密，则用 Key 去把数据 Data 进行加密，生成 Data 的密码形式(64 位)作为 DES 的输出结果；如 Mode 为解密，则用 Key 去把密码形式的数据 Data 解密，还原为 Data 的明码形式(64 位)作为 DES 的输出结果。

在通信网络的两端，双方约定一致的 Key，在通信的源点用 Key 对核心数据进行 DES 加密，然后以密码形式在公共通信网中传输到通信网络的终点，数据到达目的地后，用同样的 Key 对密码数据进行解密，便再现了明文形式的核心数据。这样就保证了核心数据在公共通信网中传输的安全性和可靠性。通过定期在通信网络的源端和目的端同时改用新 Key，便能进一步提高数据的保密性，这是现在网络金融交易的流行做法。

8.3.2 DES 算法的实现步骤

DES 算法实现需要三个步骤。DES 加密过程如图 8-4 所示。

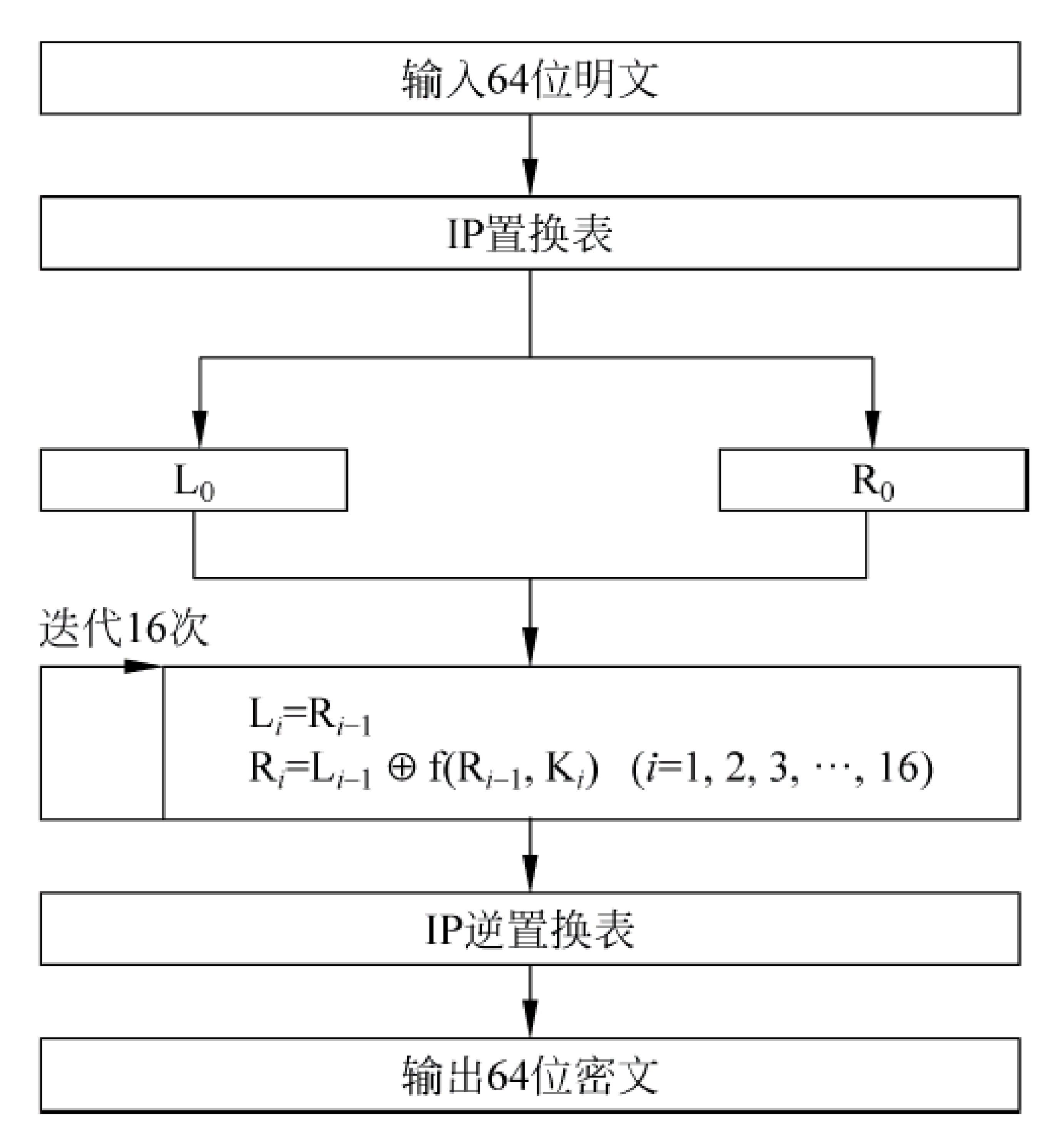


图 8-4 DES 加密过程

第 1 步：初始置换。对给定的 64 位的明文 x，首先通过一个 IP 置换表来重新排列 x，IP 置换表如表 8-1 所示，从而构造出 64 位的 x_0，$x_0=IP(x)=L_0R_0$，其中 L_0 表示 x_0 的前 32 位，R_0 表示 x_0 的后 32 位。IP 置换表如表 8-1 所示。

表 8-1 IP 置换表

58	50	12	34	26	18	10	2	60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6	64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1	59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5	63	55	47	39	31	23	15	7

其中，IP 置换过程是将输入 64 位明文的第 58 位换到第一位，第 50 位换到第二位，以此类推，最后一位是原来的第 7 位。

第 2 步：按照规则迭代(迭代 16 次)的规则为

$$L_i = R_{i-1}$$

$$R_i = L_{i-1} \oplus f(R_{i-1}, K_i) \quad (i = 1, 2, 3, \cdots, 16)$$

如果是第一次迭代 $L_1 = R_0$，$R_1 = L_0 \oplus f(R_0, K_1)$，其中符号$\oplus$表示的数学运算是异或($0\oplus0=0$，$0\oplus1=1$，$1\oplus0=1$，$1\oplus1=0$)，f 表示一种置换函数，$K_i$ 是子密钥。

1）子密钥 K_i

假设密钥为 K，长度为 64 位，但是其中第 8、16、24、32、40、48、64 位用作奇偶校验位，实际上密钥长度为 56 位。K 的下标 i 的取值范围是 1～16，用 16 轮来构造。构造过程如图 8-5 所示。

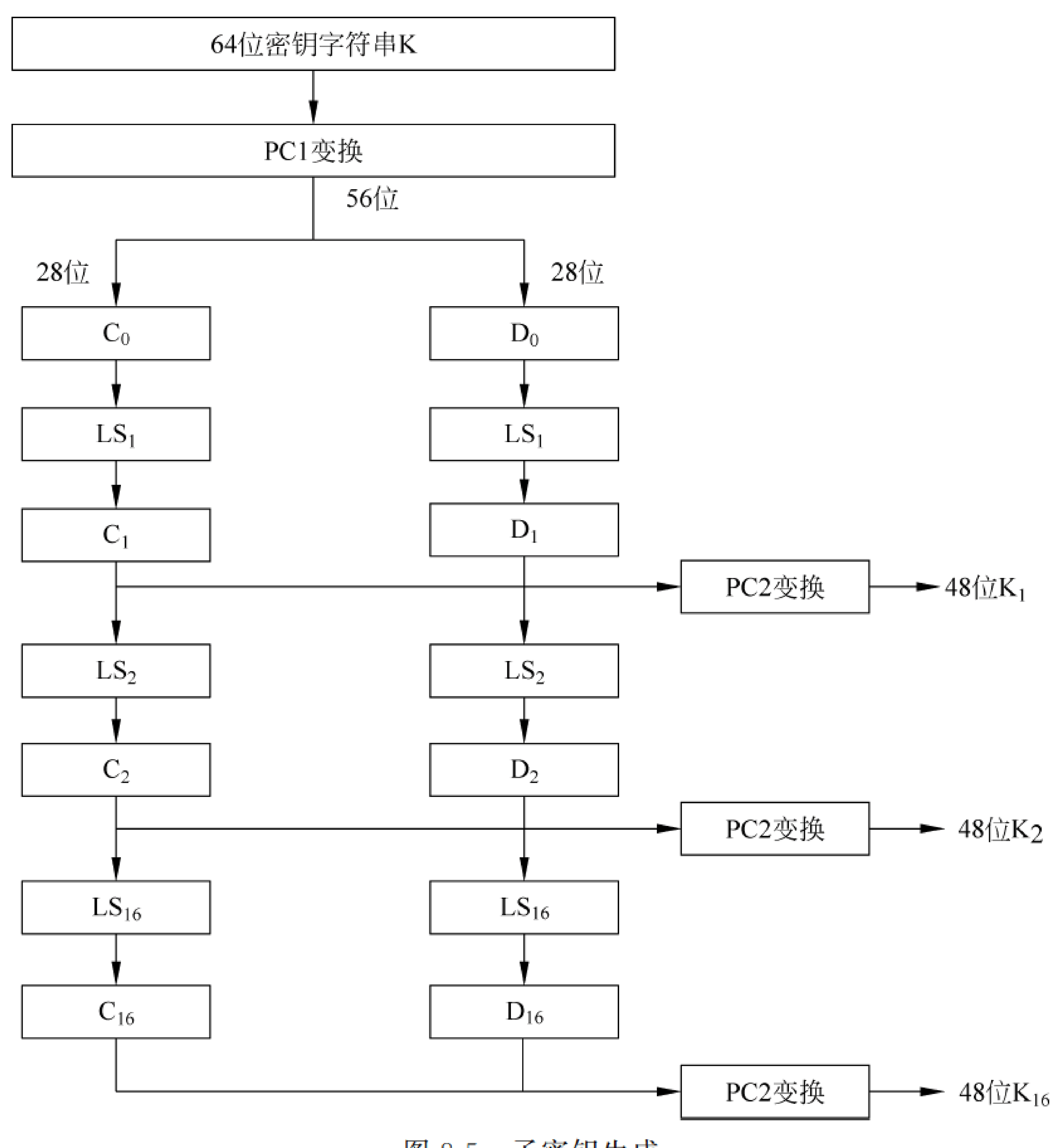


图 8-5　子密钥生成

首先，对于给定的密钥 K，应用 PC1 变换进行选位，选定后的结果是 56 位，设其前 28 位为 C_0，后 28 位为 D_0。PC1 选位如表 8-2 所示。

表 8-2　PC1 选位表

57	49	41	33	25	17	9	1	58	50	42	34	26	18
10	2	59	51	43	35	27	19	11	3	60	52	44	36
63	55	47	39	31	23	15	7	62	54	46	38	30	22
14	6	61	53	45	37	29	21	13	5	28	20	12	4

第 1 轮：第一列是 LS_1，第二列是 LS_2，以此类推。LS_1 是左移的位数。对 C_0 做左移 LS_1 得到 C_1，对 D_0 做左移 LS_1 得到 D_1，左移的原理是所有二进位循环左移。LS 移位表如表 8-3 所示。

表 8-3　LS 移位表

轮	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
位数	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

然后对 C_1D_1 应用 PC2 进行选位，得到 K_1。PC2 选位表如表 8-4 所示。

表 8-4　PC2 选位表

14	17	11	24	1	5	3	28	15	6	21	10
23	29	12	4	26	8	16	7	27	20	13	2
41	52	31	37	47	55	30	40	51	45	33	48
44	49	39	56	34	53	46	42	50	36	29	32

第 2 轮：对 C_1、D_1 做左移 LS2 得到 C_2 和 D_2，进一步对 C_2D_2 应用 PC2 进行选位，得到 K_2。如此继续，分别得到 K_3，K_4，…，K_{16}。

2）函数 f

函数 f 有两个输入：32 位的 R_{i-1} 和 48 位 K_i，f 函数的处理流程如图 8-6 所示。

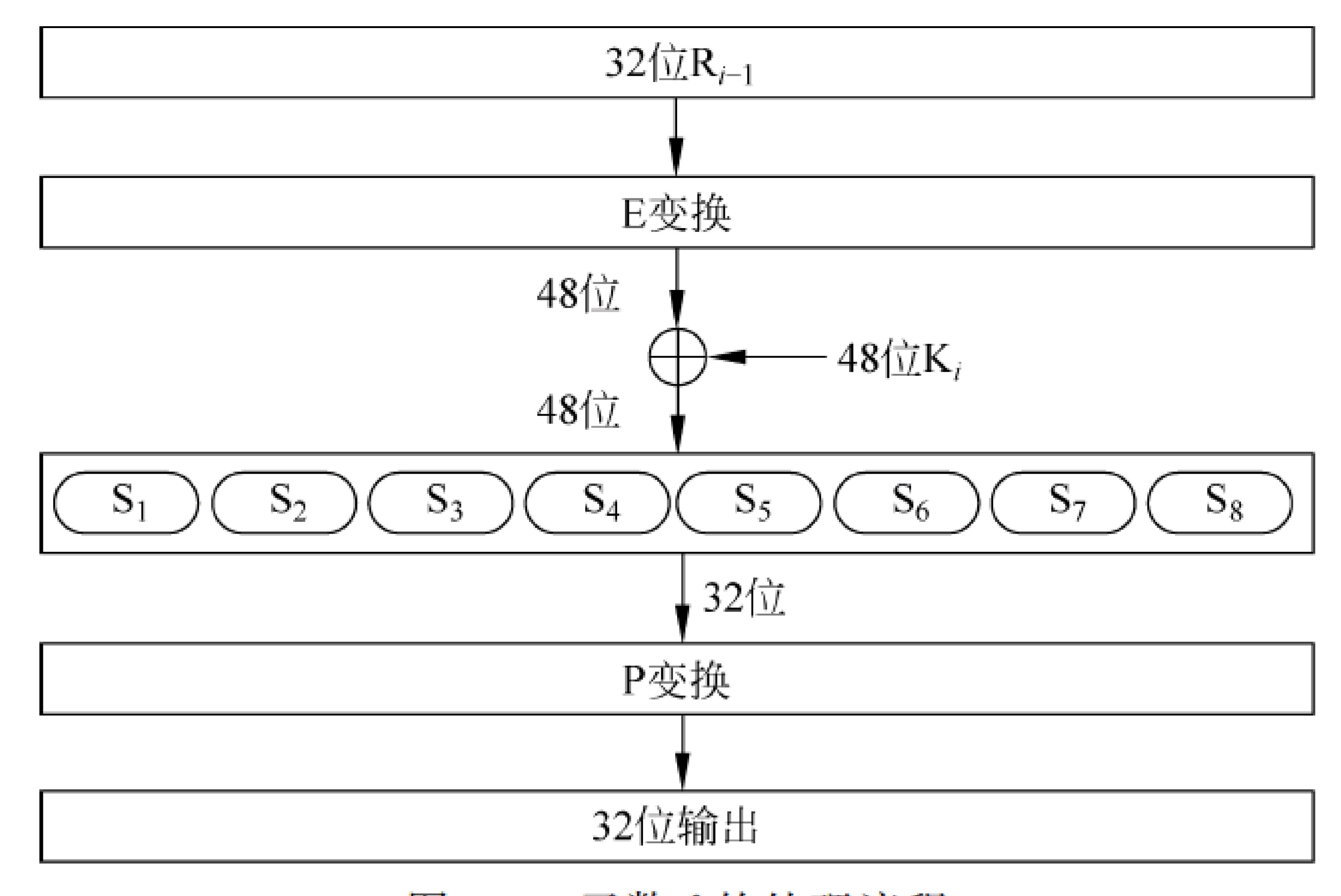


图 8-6　函数 f 的处理流程

E 变换的算法是从 R_{i-1} 的 32 位中选取某些位，构成 48 位。即 E 将 32 位扩展变换为 48 位，变换规则根据 E 位选择表，如表 8-5 所示。

表 8-5　E 位选择表

32	1	2	3	4	5	4	5	6	7	8	9	8	9	10	11
12	13	12	13	14	15	16	17	16	17	18	19	20	21	20	21
22	23	24	25	24	25	26	27	28	29	28	29	30	31	32	1

将 E 的选位结果与 K_i 做异或操作，得到一个 48 位输出。分成 8 组，每组 6 位，作为 8 个 S 盒的输入。每个 S 盒输出 4 位，共 32 位。

S 盒的工作原理是：S 盒以 6 位作为输入，而以 4 位作为输出，现在以 S1 为例说明其过程。假设输入为 $A=a_1a_2a_3a_4a_5a_6$，则 $a_2a_3a_4a_5$ 所代表的数是 0～15 之间的一个数，记为 $k=a_2a_3a_4a_5$；由 a_1a_6 所代表的数是 0～3 之间的一个数，记为 $h=a_1a_6$。在 S1 的 h 行，k 列找到一个数 B，B 在 0～15 之间，它可以用 4 位二进制表示，为 $B=b_1b_2b_3b_4$，这就是 S1 的输出。S 盒由 8 张数据表组成，如表 8-6 所示。

表 8-6　S 盒

S1															
14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13
S2															
15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9
S3															
10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12
S4															
7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14
S5															
2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3
S6															
12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13
S7															
4	11	2	15	14	0	8	13	3	12	9	7	5	10	6	1
13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12

续表

S8															
13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

例如，第 2 个 S 盒的输入为 111011。第 1 位和最后一位组合形成了 11，它对应着第 2 个盒的第三行。中间的 4 位组合在一起形成了 1101，它对应着第 2 个 S 盒的第 13 列。S 盒 2 的第三行、第 13 列就是 5(注意：行、列的记数均从 0 开始而不是从 1 开始)，则输出值是 0101。

S 盒的输出作为 P 变换的输入，P 的功能是对输入进行置换。例如，第 20 位移到第 3 位，第 25 位移到最后一位。P 换位表如表 8-7 所示。

表 8-7　P 换位表

16	7	20	21	29	12	28	17	1	15	23	26	5	18	31	10
2	8	24	14	32	27	3	9	19	13	30	6	22	11	4	25

最后，将 P 盒转换的结果与最初的 L_0 异或，然后再进行下一轮迭代。迭代 16 次以后，进入第 3 步。

第 3 步：逆置换。对 $L_{16}R_{16}$ 利用 IP^{-1} 做逆置换，就得到了密文 y。逆置换 IP^{-1} 规则表如表 8-8 所示。

表 8-8　逆置表 IP^{-1}

40	8	48	16	56	24	64	32	39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30	37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28	35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26	33	1	41	9	49	17	57	25

8.3.3　DES 算法的安全性

在 DES 作为加密标准提出后不久，学者们就开始争论 DES 的安全性。DES 的密钥长度较短，这被认为是 DES 最大的弱点。针对这个弱点的攻击包括穷举测试密钥，就是利用一个已知的明文和密文消息对进行穷举猜测，直到找到正确的密钥。

对付攻击的有效方法是用三个密钥进行三次加密。这将把已知明文攻击的工作量提高了 2^{112} 倍，这个密钥长度大大提高了抗攻击强度。其缺点是要使用 $3\times35=168$ 比特的密钥。作为替代方案，可以使用两个密钥进行的三重 DES 方案。

8.4　RSA 公钥加密技术

1978 年，Rivest、Shamir 和 Adleman 提出一种用数论构造的 RSA 算法，它是迄今为止在理论上最为成熟完善的公钥密码体制，该体制已经得到广泛的应用和实践。

8.4.1 RSA 算法的原理

RSA 算法是一种基于大数不可能质因数分解假设的公钥体系。简单地说，就是找两个很大的质数，一个公开给世界，称之为“公钥”，另一个不告诉任何人，称之为“私钥”。两个密钥互补，用公钥加密的密文可以用私钥解密，反过来也一样。假设 A 寄信给 B，他们知道对方的公钥。A 可以用 B 的公钥加密邮件寄出，B 收到后用自己的私钥解出 A 的原文，这样就保证了邮件的安全性。RSA 算法如图 8-7 所示。

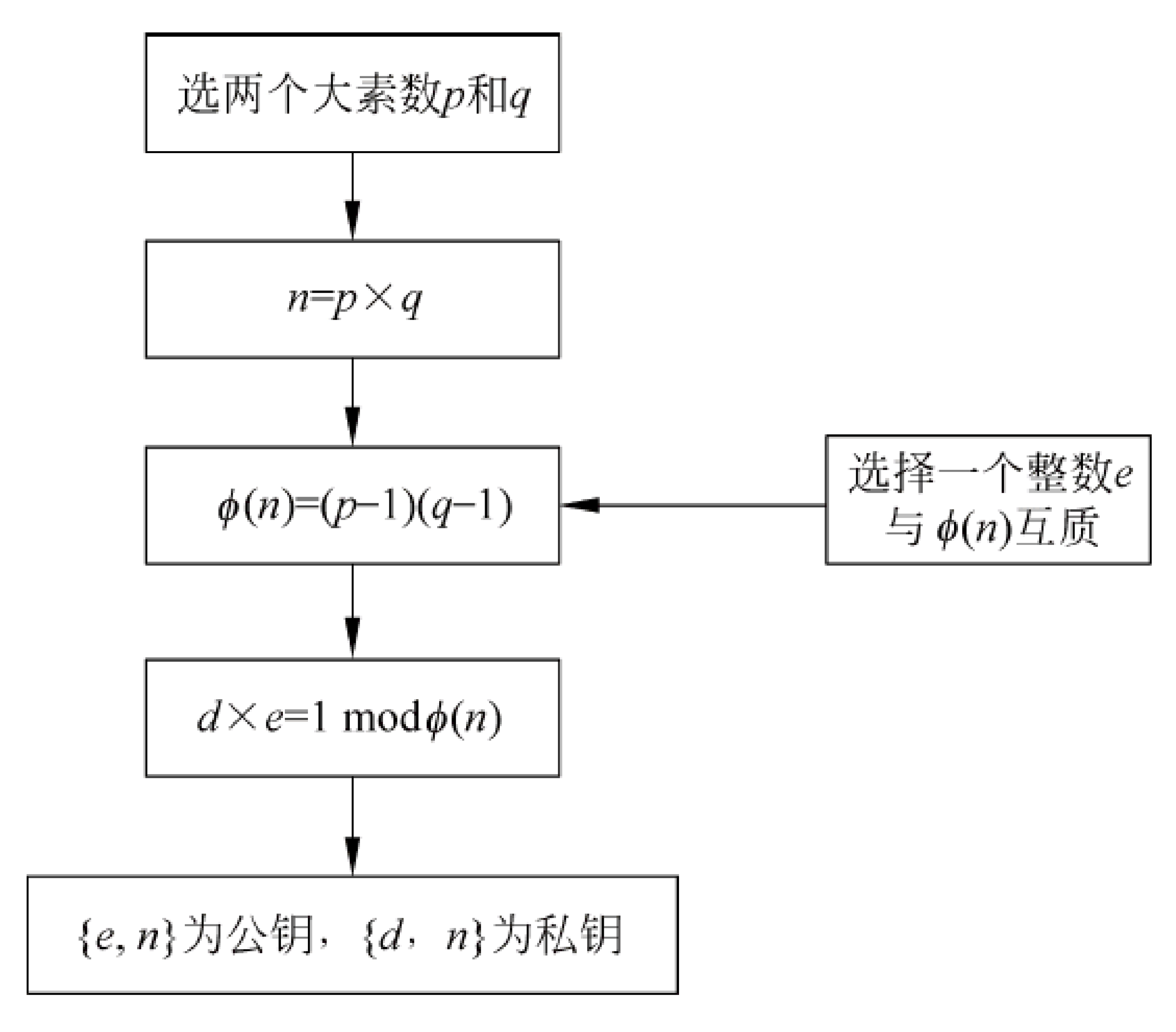


图 8-7　RSA 算法框图

1. RSA 算法的密钥的产生

(1) 选两个大素数 p 和 q。

(2) 计算这两个素数的乘积 $n=p\times q$，$\phi(n)=(p-1)(q-1)$，其中 $\phi(n)$ 是 n 的欧拉函数值。

(3) 选择一个整数 e，满足 $1<e<\phi(n)$，并且 $\gcd(e,\phi(n))=1$，也就是 e 和 $\phi(n)$ 互质。

(4) 计算 d，满足 $d\times e=1 \bmod \phi(n)$。

(5) 以 $\{e,n\}$ 为公钥，$\{d,n\}$ 为私钥。

2. RSA 算法的加密

(1) 将明文分组，使得每个分组对应的十进制数小于 n；

(2) 对每个分组明文 m，做加密运算：$c=m^e \bmod n$。

3. RSA 算法的解密

对每个分组密文，做解密运算：$m=c^d \bmod n$。

8.4.2 RSA 的安全性

RSA 算法的安全性依赖于大数分解，但是否等同于大数分解一直未能得到理论上的证明，因为没有证明破解 RSA 算法就一定需要大数分解。假设存在一种无须分解大数的算法，那它肯定可以修改成为大数分解算法。目前，RSA 算法的一些变种算法已被证明等价于大数分解，不管怎样，分解 n 是最显然的攻击方法。为了避免整数分解算法对 RSA 公钥密码系统的攻击，必须慎重选择 RSA 大整数，例如 RSA 大整数 $n=p\times q$ 必须足够大，以抵

抗数据域筛法的分解，p 与 q 的位数应差不多，以抵抗椭圆曲线算法的分解。由此可见，由于分解大整数的能力日益增强，因此为保证 RSA 体制的安全性必须增加 p 与 q 的位数。

8.4.3 RSA 与 DES 的比较

非对称加密具有更大的密钥空间或可能值范围，因此不太容易受到对每个可能密钥都进行尝试的穷举攻击。由于公钥不需要保密，因此分发起来十分容易，但条件是可通过某种其他方式来验证发送方的身份。某些非对称加密算法可用于创建数字签名，以此来验证数据发送方的身份。但是与对称加密算法相比，非对称加密的速度很慢，不适合用来加密大量数据。非对称加密算法仅对传输很少量的数据有用。非对称加密通常用于加密一个对称加密将要使用的密钥，而对会话的其余部分应用对称加密。

对称加密与非对称加密都具有各自的优点和缺点，现对两种加密算法进行比较，如表 8-9 所示。

表 8-9　DES 与 RSA 比较表

算法	密 钥 关 系	密钥传送	数字签名	速度	主 要 用 途
DES	加密密钥与解密密钥相同	不需	困难	快	数据加密
RSA	加密密钥与解密密钥不同	需要	容易	慢	数字签名、密钥加密

对称加密算法加密速度快，但密钥的管理存在安全性问题。非对称加密算法密钥管理简单，尤其是 RSA 加密算法易于理解，容易实现，安全性良好，而且已经有大量针对 RSA 算法的改进方法可以应用。

8.5 信息加密技术应用

在网络安全领域，网络数据加密是解决通信网络中信息安全的有效方法。常用的网络数据加密方式主要有链路加密、节点加密和端到端加密。

8.5.1 链路加密

链路加密是对网络中两个相邻节点之间传输的数据进行加密保护，如图 8-8 所示。对于链路加密，所有消息在被传输之前进行加密，在每一个节点对接收到的消息进行解密后，先使用下一链路的密钥对消息进行加密，再进行传输。在到达目的地之前，一条消息可能要经过多条通信链路的传输。

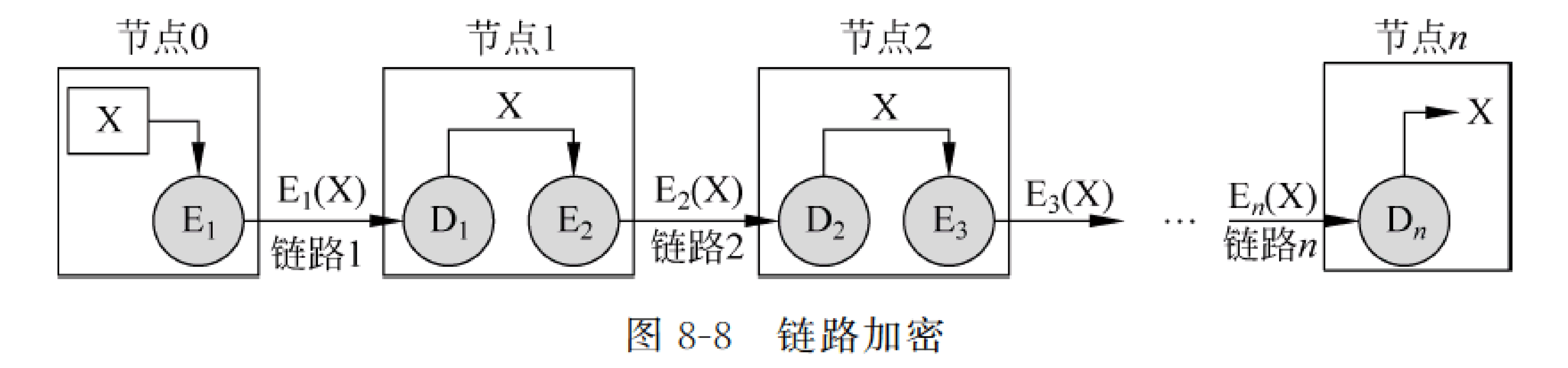


图 8-8　链路加密

由于在每一个中间传输节点，消息均被解密后重新进行加密，因此包括路由信息在内的链路上的所有数据均以密文形式出现。所以链路加密就掩盖了被传输消息的源点与终点。

由于填充技术的使用及填充字符在不需要传输数据的情况下就可以进行加密，这使得消息的频率和长度特性得以掩盖，从而可以防止对通信业务进行分析。

尽管链路加密在计算机网络环境中广泛使用，但也存在一些问题。链路加密通常用在点对点的同步或异步线路上，它要求先对链路两端的加密设备进行同步，然后使用一种链模式对链路上传输的数据进行加密，这就给网络的性能和可管理性带来了副作用。在线路信号连通性不好的海外或卫星网络中，链路上的加密设备需要频繁地进行同步，其带来的后果是数据丢失或重传。因此，即使一小部分数据需要进行加密，也会使得所有传输数据重新加密。

在一个网络节点，链路加密仅在通信链路上提供安全性，消息以明文形式存在，因此所有节点在物理上必须是安全的，否则就会泄漏明文内容。在传统的单钥加密算法中，解密密钥与加密密钥是相同的，该密钥必须被秘密保存，并按一定规则进行变化。因此，密钥分配的链路要对密钥进行物理传送或者建立专用网络设施。网络节点地理分布的广阔性使得这一过程变得复杂，同时增加了密钥连续分配时的代价。

8.5.2 节点加密

节点加密是指在信息传输路过的节点处进行解密和加密。尽管节点加密能给网络数据提供较高的安全性，但它在操作方式上与链路加密是类似的，两者均在通信链路上为传输的信息提供安全保障，都在中间节点先对信息进行解密，然后进行加密。因为要对所有传输的数据进行加密，所以加密过程对用户是透明的。然而与链路加密不同的是，节点加密不允许信息在网络节点以明文形式存在，它先把收到的信息进行解密，然后采用另一个不同的密钥进行加密，这一过程是在节点上的一个安全模块中进行的。

节点加密要求报头和路由信息以明文形式传输，以便中间节点能得到如何处理信息的指示，因此这种方法对于防止攻击者分析通信业务是脆弱的。

8.5.3 端到端加密

端到端加密是指对一对用户之间的数据连续地提供保护，如图 8-9 所示。端到端加密允许数据在从源点到终点的传输过程中始终以密文形式存在。采用端到端加密，信息在被传输到达终点之前不进行解密，因为信息在整个传输过程中均受到保护，所以即使有节点被损坏也不会使信息泄漏。

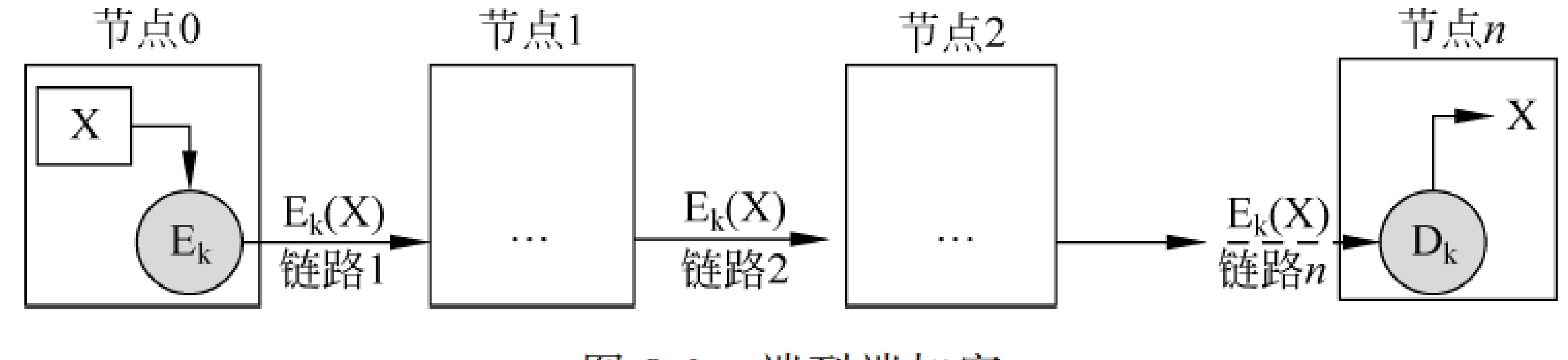
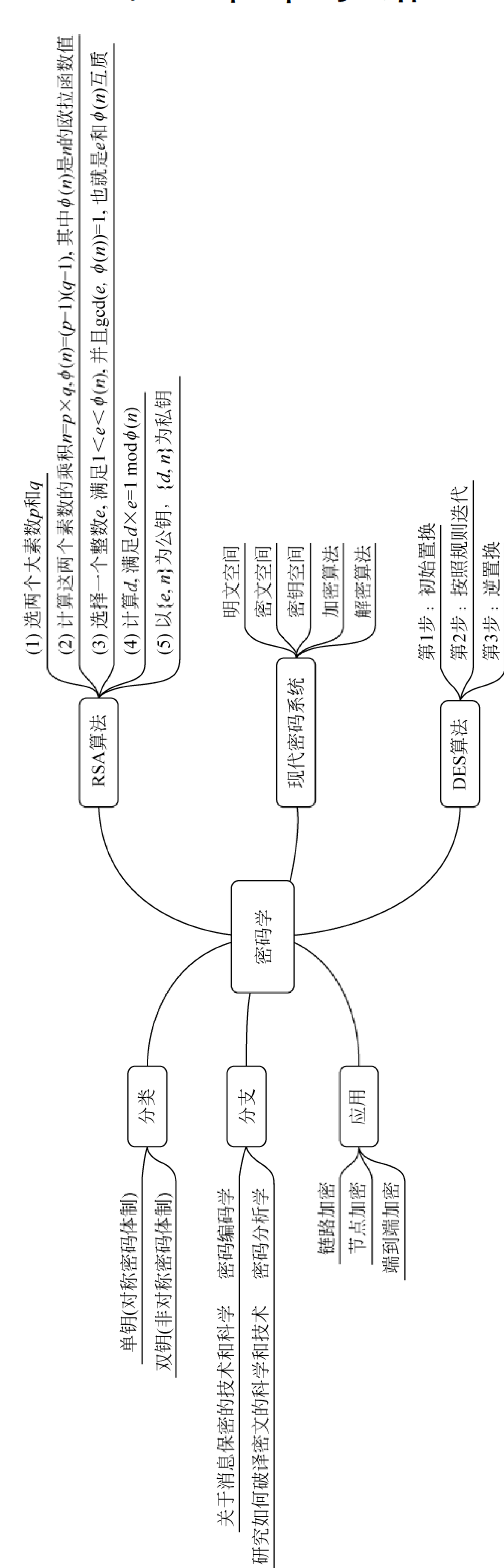


图 8-9　端到端加密

端到端加密系统的价格便宜，且与链路加密和节点加密相比更可靠，更容易设计、实现和维护。端到端加密还避免了其他加密系统所固有的同步问题，因为每个报文包均是独立被加密的，所以一个报文包所发生的传输错误不会影响后续的报文包。

端到端加密系统通常不允许对信息的目的地址进行加密，这是因为每一个信息所经过的节点都要用此地址来确定如何传输信息。由于这种加密方法不能掩盖被传输信息的源点与终点，因此它对于防止攻击者分析通信业务也是脆弱的。

8.6 本章小结


密码学
RSA算法
(1) 选两个大素数p和q
(2) 计算这两个素数的乘积n=p×q, φ(n)=(p−1)(q−1), 其中φ(n)是n的欧拉函数值
(3) 选择一个整数e, 满足1<e<φ(n), 并且gcd(e, φ(n))=1, 也就是e和φ(n)互质
(4) 计算d, 满足d×e=1 mod φ(n)
(5) 以{e, n}为公钥，{d, n}为私钥
现代密码系统
明文空间
密文空间
密钥空间
加密算法
解密算法
DES算法
第1步：初始置换
第2步：按照规则迭代
第3步：逆置换
分类
单钥(对称密码体制)
双钥(非对称密码体制)
分支
密码编码学
关于消息保密的技术和科学
密码分析学
研究如何破译密文的科学和技术
应用
链路加密
节点加密
端到端加密

8.7 习　　题

一、填空题

1. 现代密码系统也称为密码体制，一般由 5 个部分组成，包括明文空间、密文空间、(　　)、加密算法和解密算法。

2. 密码体制从原理上可分为两大类，即(　　)和非对称密码体制。

3. 对称加密技术对信息的加密与解密都使用相同的密钥，因此又称为(　　)技术。

4. DES 算法采用了(　　)位密钥长度，其中 8 位用于奇偶校验。

5. 非对称加密技术对信息的加密与解密使用不同的密钥，用来加密的密钥是可以公开的公钥，用来解密的密钥是需要保密的私钥，因此又被称为(　　)技术。

二、选择题

1. 以下关于对称密钥加密说法正确的是(　　)。

A. 加密方和解密方可以使用不同的算法

B. 加密密钥和解密密钥可以是不同的

C. 加密密钥和解密密钥必须是相同的

D. 密钥的管理非常简单

2. 以下关于非对称密钥加密说法正确的是(　　)

A. 加密方和解密方使用的是不同的算法　　B. 加密密钥和解密密钥是不同的

C. 加密密钥和解密密钥匙是相同的　　D. 加密密钥和解密密钥没有任何关系

3. 以下关于混合加密方式说法正确的是(　　)。

A. 采用公开密钥体制进行通信过程中的加解密处理

B. 采用公开密钥体制对对称密钥体制的密钥进行加密后的通信

C. 采用对称密钥体制对对称密钥体制的密钥进行加密后的通信

D. 采用混合加密方式，利用了对称密钥体制的密钥容易管理和非对称密钥体制的加解密处理速度快的双重优点

4. 利用 3DES 进行加密，以下说法正确的是(　　)。

A. 3DES 的密钥长度是 56 位

B. 3DES 全部使用三个不同的密钥进行三次加密

C. 3DES 的安全性高于 DES

D. 3DES 的加密速度比 DES 加密速度快

5. DES 算法中扩展运算 E 的功能是(　　)。

A. 对 16 位的数据组的各位进行选择和排列，产生一个 32 位的结果

B. 对 32 位的数据组的各位进行选择和排列，产生一个 48 位的结果

C. 对 48 位的数据组的各位进行选择和排列，产生一个 64 位的结果

D. 对 56 位的数据组的各位进行选择和排列，产生一个 64 位的结果

6. S 盒是 DES 中唯一的非线性部分，DES 的安全强度主要取决于 S 盒的安全程序。DES 中有(　　)个 S 盒，其中(　　)。

A. 2　　B. 4　　C. 6　　D. 8

E. 每个 S 盒有 6 个输入，4 个输出　　F. 每个 S 盒有 4 个输入，6 个输出

G. 每个 S 盒有 48 个输入，32 个输出　　H. 每个 S 盒有 32 个输入，48 个输出

7. 若 Bob 给 Alice 发送一封邮件，并想让 Alice 确信邮件是由 Bob 发出的，则 Bob 应该选用(　　)对邮件加密。

A. Alice 的公钥　　B. Alice 的私钥　　C. Bob 的公钥　　D. Bob 的私钥

8. DES 算法的特点是，密钥是固定的 56 位，并且加密的数据必须是以(　　)的块为单位进行加密的。

A. 32 位　　B. 56 位　　C. 64 位　　D. 72 位

9. 在密码学中，下列对 RSA 的描述正确的是(　　)。

A. RSA 是秘密密钥算法和对称密钥算法

B. RSA 是非对称密钥算法和公钥算法

C. RSA 是秘密密钥算法和非对称密钥算法

D. RSA 是公钥算法和对称密钥算法

10. 表 8-10 是 DES 算法中 S4 盒的选择矩阵，如果其输入为 101011，输出的是(　　)。

表　8-10

7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14

A. 0001　　B. 0100　　C. 1010　　D. 0011

11. 表 8-11 是 DES 算法中 S4 盒的选择矩阵，如果其输入为 110011，输出的是(　　)。

表　8-11

7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14

A. 0001　　B. 0100　　C. 1010　　D. 0011

三、判断题

1. 密码编码学是密码体制的设计学，即采用什么样的密码体制保证信息被安全地加密。从事此行业的人员被称为密码编码者。

2. 根据被破译的难易程度，不同的密码算法具有不同的安全等级。如果破译算法的代价大于加密数据的价值，那么算法可能是安全的。

3. 密钥是保密通信安全的关键，发信方必须安全、妥善地把密钥护送到收信方，不能泄漏其内容。如何才能把密钥安全地送到收信方，是公钥密码算法的突出问题。

4. DES 算法是目前广泛采用的对称加密方式之一，加密和解密使用同一种算法，加密

和解密时的密钥也是相同的。

5. 非对称加密技术中,用来加密的公钥与解密的私钥是数学相关的,并且加密公钥与解密私钥是成对出现的,但是不能通过加密公钥来计算出解密私钥。

6. 公钥加密体制的优点是可以公开加密密钥,适应网络的开放性要求,且仅需保密解密密钥。其主要缺点是加密算法复杂,加密与解密的速度比较慢。

7. RSA 算法是一种基于大数不可能质因数分解假设的公钥体系。

8. 对称加密算法加密速度快,但密钥的管理存在安全性问题;非对称加密算法密钥管理简单,但加密速度慢。

四、简答题

1. 什么是密钥?

2. 什么是明文?

五、综合题

1. 在 RSA 算法中,选择两个素数 $p=5$,$q=11$,加密密钥为 $e=3$,假设需要加密的明文信息为 $m=3$。

(1) 计算出解密密钥 d;

(2) 说明使用 RSA 算法的加密过程及结果?

2. 假设需要加密的明文信息为 $m=4$,选择 $p=5$,$q=11$,$e=7$,试使用 RSA 算法求解公钥、私钥和加密结果 c 的值。

第 9 章 无线网络安全

【本章学习目标】

- 了解无线网络
- 了解无线网络面临的安全威胁
- 理解物理地址过滤技术
- 理解服务区标识符匹配技术
- 掌握 WEP 加密解密过程

9.1 无线网络概述

9.1.1 无线局域网

无线局域网(WLAN)提供了移动接入的功能,这给许多需要发送数据但又不能坐在办公室的工作人员提供了方便。当要求大量持有便携式计算机的用户在同一个地方同时上网时(如在临时会议的地点、野外等),如果采用电缆连网,布线是很大的问题,这时采用无线局域网就比较容易。无线局域网还有投资少、建网速度快等优点。

无线局域网是计算机网络与无线通信技术相结合的产物。它利用射频(RF)技术,取代旧式的双绞铜线构成局域网,提供传统有线局域网的所有功能。

无线局域网的发展经历了两个阶段：IEEE 802.11 标准出台以前各个标准互不兼容的阶段和 IEEE 802.11 标准问世以后的无线网络产品规范化阶段。IEEE 802.11 标准代表了无线网所需要具备的特点。无线局域网有两种配置方案：有基站及没有基站。IEEE 802.11 标准对这两种方案都提供了支持,凡是使用 IEEE 802.11 系列协议的局域网又称为 Wi-Fi (Wireless-Fidelity)。

1. IEEE 802.11 基站结构模型

IEEE 802.11 标准规定无线局域网的最小构件是基本服务集(Basic Service Set,BSS)。一个基本服务集包括一个基站(base station)和若干个使用相同 MAC 协议共享媒体的移动站,所有移动站在本 BSS 以内都可以直接通信,但在和本 BSS 以外的移动站通信时都必须通过本 BSS 的基站。基本服务集内的基站就是接入点(Access Point,AP)。

一个基本服务集可以是孤立的,也可通过接入点连接到一个分配系统(Distribution System,DS),然后再连接到另一个基本服务集,这样就构成了一个扩展的服务集(Extended Service Set,ESS)。分配系统可以使用以太网(这是最常用的)、点对点链路或其他无线网

络。扩展服务集可以为无线用户提供到有线局域网的接入。这种接入是通过无线网桥来实现的。

2. 自组网络

没有基站的无线局域网又叫作自组网络(ad hoc network)。这种自组网络没有上述基本服务集中的接入点,而是由一些处于平等状态的站之间相互通信组成的临时网络。在自组网络中,源节点和目的节点之间的其他节点为转发节点,这些节点都具有路由器的功能。由于自组网络没有预先建好的网络固定基础设施(基站),因此自组网络的服务范围通常是受限的,而且自组网络一般也不和外界的其他网络相连接。自组网络有很好的应用前景,例如战场指挥、灾害场景、移动会议、传感器网络等。

近年来,无线传感器网络(Wireless Sensor Network,WSN)引起了人们广泛的关注。无线传感器网络是由大量传感器节点通过无线通信技术构成的自组网络。无线传感器网络的应用就是进行各种数据的采集、处理和传输,它一般并不需要很高的带宽,但是在大部分时间必须保持低功耗,以节省电池的消耗。由于无线传感节点的存储容量有限,因此对协议栈的大小有严格的限制。

3. IEEE 802.11 服务

IEEE 802.11 定义了标准无线 LAN 必须提供的 9 种服务。这些服务可以分成两类:5 种分发服务和 4 种站服务。分发服务涉及对 BSS 的成员关系的管理,并且会影响到 BSS 之外的站。与之相反,站服务则只与一个 BSS 内部的活动有关系。

1) 分发服务

5 种分发服务是由基站提供的,它们处理站的移动性。当移动站进入 BSS 的时候,通过这些服务与基站关联起来;当移动站离开 BSS 的时候,通过这些服务与基站断开联系。这 5 种分发服务如下。

(1) 关联(association)。移动站利用该服务连接到基站上。典型情况下,当一个移动站进入到一个基站的无线电距离范围之内时,这种服务就会被用到。

(2) 分离(disassociation)。不管是移动站,还是基站,都有可能会解除关联关系。一个站在离开或者关闭之前,先使用这项服务;基站在停下来进行维护之前也可能会用到该服务。

(3) 重新关联(reassociation)。利用这项服务,一个站可以改变它的首选基站。这项服务对于那些从一个 BSS 移动到另一个 BSS 的移动站来说,是非常有用的。

(4) 分发(distribution)。这项服务决定了如何路由那些发送给基站的帧。如果帧的目标对于基站来说是本地的,则该帧将被直接发送到空中,否则它们必须通过 DS 来转发。

(5) 融合(integration)。如果一帧需要通过一个非 IEEE 802.11 的网络来发送,并且该网络使用了不同的编址方案或者不同的帧格式,则通过这项服务可以将 IEEE 802.11 格式的帧翻译成目标网络所要求的帧格式。

2) 站服务

4 种站服务都是在 BSS 内部进行的。当关联过程完成之后,这些服务才可能会用到。这 4 种服务如下。

(1) 认证(authentication)。因为未授权的站很容易就可以发送或者接收无线通信流

量，所以，任何一个站必须首先证明自己的身份，然后才允许发送数据。典型情况下，当基站接受了一个移动站的关联请求之后，基站将给它发送一个特殊的质询帧，以确定该移动站是否知道原先分配给它的密钥（口令）；移动站加密质询帧并送回给基站，如果结果正确，就可以证明它是知道密钥的，移动站就会被全接纳。

（2）解除认证（deauthentication）。如果一个原先已经通过认证的移动站要离开网络，则它需要解除认证。

（3）私密性（privacy）。如果在无线 LAN 上发送的信息需要保密，则它必须被加密。这项服务管理加密和解密。

（4）数据投递（data delivery）。最后，真正的目的是为了传输数据，所以，IEEE 802.11 必须提供一种传送和接收数据的方法。IEEE 802.11 的传输过程不保证可靠性，上面的层必须处理检错和纠错工作。

9.1.2 无线个域网

无线个域网（Wireless Personal Area Network，WPAN）是当前计算机网络发展最为迅速的领域之一。WPAN 就是在个人工作或生活的地方把属于个人使用的电子设备（如便携式电脑、掌上电脑、便携式打印机以及蜂窝电话等）用无线技术连接起来的自组网络。WPAN 可以是一个人使用，也可以是若干人共同使用（例如，一个教研室的几位教师把几米范围内使用的一些电子设备组成一个无线个人区域网）。这些电子设备可以很方便地进行通信，并且解决了使用导线的麻烦。

WPAN 的 IEEE 标准都由 IEEE 802.15 工作组制定，这个标准也是包括 MAC 层和物理层的标准。WPAN 都工作在 2.4GHz 的 ISM 频段。WPAN 被广泛关注的技术及其标准有以下三个。

1. IEEE 802.15.1

IEEE 802.15.1 覆盖了蓝牙（Bluetooth）协议栈的物理层/媒体接入控制层（PHY/MAC）。

1998 年 5 月，5 家世界著名的 IT 公司（爱立信、IBM、英特尔、诺基亚和东芝）联合宣布了“蓝牙”计划，使不同厂家的便携设备在没有电缆连接时，利用无线技术在近距离范围内具有相互操作的性能。随后这 5 家公司组建了一个特殊的兴趣组织（SIG）来负责此项计划的研发。这项计划一经公布，就得到了包括摩托罗拉、朗讯、康柏、西门子以及微软等大公司在内的近 2000 家厂商的广泛支持和采纳。1999 年 7 月蓝牙 SIG 推出了蓝牙协议 1.0 版。

IEEE 802.15.1 标准是由 IEEE 与蓝牙 SIG 共同合作完成的，其源于蓝牙 v1.1 版，并已于 2002 年 4 月 15 日由 IEEE-SA 的标准部门批准成为一个正式标准，它可以同蓝牙 v1.1 完全兼容。

IEEE 802.15.1 是用于 WPAN 的无线媒体接入控制层和物理层规范。标准的目标是在个人操作空间（POS）内进行无线通信。

2. IEEE 802.15.3a

IEEE 802.15.3a 是超宽带（Ultra-Wide Band，UWB）标准。

超宽带技术起源于 20 世纪 50 年代末，此前主要作为军事技术在雷达探测和定位等应

用领域中使用。美国联邦通信委员会(FCC)于2002年2月准许该技术进入民用领域,用户不必进行申请即可使用。作为室内通信所采用的技术,FCC已将3.1～10.6GHz频带向UWB通信开放。

传统的"窄带"和"宽带"都是采用无线电频率(RF)载波来传送信号,利用载波的状态变化来传输信息。而超宽带是基带传输,通过发送代表0和1的脉冲无线电信号来传送数据。这些脉冲信号的时域极窄(纳秒级),频域极宽(数Hz到数GHz,甚至超过10GHz),其中的低频部分可以实现穿墙通信。

关于UWB技术主要有两种相互竞争的标准:以Intel和Texas Instrument为代表的MBOA标准,主张采用多频带方式来实现UWB技术;以Motorola为代表的DS-UWB标准,主张采用单频带方式来实现UWB技术。

UWB技术有如下几个突出特点:

(1) 超宽带技术使用了瞬间高速脉冲,因此信号的频带很宽,可支持100～400Mb/s的数据率。可用于小范围内高速传送图像或DVD质量的多媒体视频文件。

(2) UWB只在需要传输数据时才发送脉冲,信号的功率谱密度极低,发射系统比现有的传统无线电技术功耗低得多。在高速通信时系统的耗电量仅为几百微瓦(μW)至几十毫瓦(mW)。民用的UWB设备功率一般是传统移动电话所需功率的1/100左右,是蓝牙设备所需功率的1/20左右,因此,UWB设备在电池寿命和电磁辐射上,相对于传统无线设备有着很大的优越性。

(3) 由于UWB的脉冲非常短,频段非常宽,因此能避免多路径传输的信号干扰问题。同时短而弱的脉冲也使UWB与其他无线通信技术间产生干扰的可能性大幅降低,因此可与其他技术共存。

(4) 由于UWB信号射频带宽可以达到1GHz以上,它的发射功率谱密度很低,信号隐蔽在环境噪声和其他信号之中,用传统的接收机无法接收和识别,必须采用与发送端一致的扩频码脉冲序列才能进行解调,因此增加了系统的安全性。

3. IEEE 802.15.4

IEEE 802.15.4(Low-Rate Wireless Personal Area Network,LR-WPAN,低速无线个域网),覆盖了ZigBee协议栈的物理层/媒体接入控制层(PHY/MAC)。

IEEE 802.15.4标准主要针对低速无线个域网制定。该标准把低能量消耗、低速率传输、低成本作为重点目标。ZigBee标准是在IEEE 802.15.4标准基础上发展而来的。IEEE 802.15.4定义了ZigBee协议栈的最低的两层(物理层和MAC层),上面的两层(网络层和应用层)则是由ZigBee联盟定义的。

ZigBee技术主要用于各种电子设备(固定的、便携的和移动的)之间的无线通信,其主要特点是通信距离短(10～100m),传输数据速率低、功耗低,并且成本低廉。ZigBee技术有如下主要优点。

(1) 省电(功耗低)。两节五号电池支持长达6个月至2年左右的使用时间。

(2) 可靠。采用了碰撞避免机制,同时为需要固定带宽的通信业务预留了专用时隙,避免了发送数据时的竞争和冲突。节点模块之间具有自动动态组网的功能,信息在整个ZigBee网络中通过自动路由的方式进行传输,从而保证了信息传输的可靠性。

(3) 延迟短。针对延迟敏感的应用做了优化,通信延迟和从休眠状态激活的延迟都非常短。

(4) 网络容量大。可支持达 65 000 个节点。

(5) 安全性和高保密性。ZigBee 提供了数据完整性检查和鉴别功能,加密算法采用通用的 AES-128。

9.1.3 无线城域网

20 世纪 90 年代,宽带无线接入技术快速发展起来,但是相关市场一直没有繁荣扩大,一个很重要的原因就是没有统一的全球性标准。1999 年,IEEE 成立了 IEEE 802.16 工作组来专门研究宽带固定无线接入技术规范,目标就是要建立一个全球统一的宽带无线接入标准。为了促进达成这一目的,几家世界知名企业还发起成立了 WiMAX(World Interoperability for Microwave Access)论坛,力争在全球范围推广这一标准。IEEE 802.16 的出现大大地推动了宽带无线接入技术在全球的发展,特别是 WiMAX 论坛的发展壮大,强烈地刺激了市场的发展。

近年来无线城域网(WMAN)又成为无线网络中的一个热点,可提供"最后一英里"的宽带无线接入(固定的、移动的和便携的)。在许多情况下,无线城域网可用来代替现有的有线宽带接入,因此它有时又称为无线本地环路(wireless local loop)。

现在无线城域网共有两个正式标准。一个是 2004 年 6 月通过的 IEEE 802.16 的修订版本,即 IEEE 802.16d,是固定宽带无线接入空中的接口标准(2~66GHz 频段)。另一个是 2005 年 12 月通过的 IEEE 802.16 的增强版本,即 IEEE 802.16e,是支持移动性的宽带无线接入空中的接口标准(2~6GHz 频段),在其频段上它向下兼容 IEEE 802.16d。

9.2 无线网络面临的安全威胁

1. 窃听

无线网络易遭受匿名黑客的攻击,攻击者可以截获无线电信号并解析出数据。用于无线窃听的设备与用于无线网络接入的设备相同,这些设备经过很小的改动就可以被设置成截获特定无线信道或频率数据的设备。这种攻击行为几乎不可能被检测到。通过使用无线网络,攻击者可以在距离目标很远的地方进行攻击。窃听主要用于收集目标网络的信息,包括谁在使用网络、能访问什么信息及网络设备的性能等。很多常用协议通过明文传送用户名和密码等敏感信息,使攻击者可以通过截获数据获得对网络资源的访问。即使通信被加密,攻击者仍可收集加密信息用于以后的分析。很多加密算法很容易被破解。如果攻击者可以连接到无线网络上,他还可以使用 ARP 欺骗进行主动窃听。ARP 欺骗实际上是一种作用在数据链路层的中间人攻击,攻击者通过给目标主机发送 ARP 欺骗数据包来旁路通信。当攻击者收到目标主机的数据后,再将它转发给真正的目标主机。这样,攻击者可以窃听无线网络或有线网络中主机间的通信数据。

2. 通信阻断

有意或无意的干扰源可以阻断通信。对整个网络进行 DoS 攻击可以造成通信阻断,使

包括客户端和基站在内的整个区域的通信线路堵塞，造成设备之间不能正常通信。针对无线网络的 DoS 攻击很难预防。此外，大部分无线网络通信都采用公共频段，很容易受到来自其他设备的干扰。攻击者可以采用客户端阻断和基站阻断方式来阻断通信。攻击者可能通过客户端阻断占用或假冒被阻断的客户端，也可能只是对客户端发动 DoS 攻击；攻击者可能通过基站阻断假冒被阻断的基站。如前所述，有很多设备都采用公共频道进行通信，他们都可以对无线网络形成干扰。所以在部署无线网络前，电信运营商一定要进行站点调查，以验证现有设备不会对无线网络形成干扰。

3. 数据的注入和篡改

黑客通过向已有连接中注入数据来截获连接或发送恶意数据和命令。攻击者能够通过基站插入数据或命令来篡改控制信息，造成用户连接中断。数据注入可被用作 DoS 攻击。攻击者可以向网络接入点发送大量连接请求包，使接入点用户连接数超标，以此造成接入点拒绝合法用户的访问。如果上层协议没有提供实时数据完整性检测，在连接中注入数据也是可能的。

4. 中间人攻击

中间人攻击与数据注入攻击类似，所不同的是它可以采取多种形式，主要是为了破坏会话的机密性和完整性。中间人攻击比大多数攻击更复杂，攻击者需要对网络有深入的了解。攻击者通常伪装成网络资源，当受害者开始建立连接时，攻击者会截取连接，并与目的端建立连接，同时将所有通信经攻击主机代理到目的端。这时，攻击者就可以注入数据、修改通信数据或进行窃听攻击。

5. 客户端伪装

通过对客户端的研究，攻击者可以模仿或克隆客户端的身份信息，以试图获得对网络或服务的访问。攻击者也可以通过窃取的访问设备来访问网络。要保证所有设备的物理安全非常困难，当攻击者通过窃取的设备发起攻击时，通过第 2 层访问控制手段来限制对资源的访问都将失去作用。

6. 接入点伪装

高超的攻击者可以伪装接入点。客户端可能在未察觉的情况下连接到该接入点，并泄露机密认证信息。这种攻击方式可以与上面描述的接入点通信阻断攻击方式结合起来使用。

7. 匿名攻击

攻击者可以隐藏在无线网络覆盖的任何角落，并保持匿名状态，这使定位和犯罪调查变得异常困难。一种常见的匿名攻击称为沿街扫描，指攻击者在特定的区域扫描并搜寻开放的无线网络。这个名称来自一种古老的拨号攻击方式——沿街扫描，即通过拨打不通的电话号码来查找 Modem 或其他网络入口。值得注意的是，许多攻击者发动匿名攻击不是为了攻击无线网络本身，只是为了找到接入因特网并攻击其他主机的跳板。因此，随着匿名接入者的增多，针对因特网的攻击也会增加。

8. 客户端对客户端的攻击

在无线网络上，一个客户端可以对另一客户端进行攻击。没有部署个人防火墙或进行加固的客户端如果受到攻击，很可能会泄露用户名和密码等机密信息。攻击者可以利用这些信息获得对其他网络资源的访问权限。在对等模式下，攻击者可以通过发送伪造路由协

议报文以产生通路循环来实施拒绝服务攻击,或者通过发送伪造路由协议报文生成黑洞(接收和扔掉数据报文)来实现各种形式的攻击。

9. 隐匿无线信道

网络的部署者在设计和评估网络时,需要考虑隐匿无线信道的问题。由于硬件无线接入点的价格逐渐降低,以及可以通过在装有无线网卡的机器上安装软件来实现无线接入点的功能,隐匿无线信道的问题日趋严重。网络管理员应该及时检查网络上存在的一些设置有问题或非法部署的无线网络设备。这些设备可以在有线网络上制造黑客入侵的后门,使攻击者可以在距离网络很远的地点实施攻击。

10. 服务区标识符的安全问题

服务区标识符(SSID)是无线接入点用于标识本地无线子网的标识符。如果一个客户端不知道服务区标识符,接入点会拒绝该客户端对本地子网的访问。当客户端连接到接入点上时,服务区标识符的作用相当于一个简单的口令,起到一定的安全防护作用。如果接入点被设置成对 SSID 进行广播,那么所有的客户端都可以接收到它并用其访问无线网络。而且,很多接入点都采用出厂时默认设置的 SSID 值,黑客很容易通过因特网查到这些默认值。黑客获得这些 SSID 值后,就可以对网络实施攻击。因此,SSID 不能作为保障安全的主要手段。

11. 漫游造成的问题

无线网络与有线网络的主要区别在于无线终端的移动性。在 CDMA、GSM 和无线以太网中,漫游机制都是相似的。很多 TCP/IP 服务都要求客户端和服务端的 IP 地址保持不变,但是,当用户在网络中移动时,不可避免地会离开一个子网而加入另一个子网,这就要求无线网络提供漫游机制。移动 IP 的基本原理在于地点注册和报文转发,一个与地点无关的地址用于保持 TCP/IP 连接,而另一个随地点变化的临时地址用于访问本地网络资源。在移动 IP 系统中,当一个移动节点漫游到一个网络时,就会获得一个与地点有关的临时地址,并注册到外地代理上。外地代理会与所属地代理联系,通知所属地代理有关移动节点的接入情况。所属地代理将所有发往移动节点的数据包转发到外地代理上。这种机制会带来一些问题:首先,攻击者可以通过对注册过程的重放来获取发送到移动节点的数据;其次,攻击者也可以模拟移动节点以非法获取网络资源。

9.3 无线局域网安全技术

无线局域网的安全技术包括物理地址(MAC 地址)过滤,服务区标识符(SSID)匹配,连线对等保密(WEP)等。

9.3.1 物理地址过滤

每个无线客户端网卡都由唯一的 48 位物理地址(MAC 地址)标志,可在 AP 中手工维护一组允许访问的 MAC 地址列表,实现物理地址过滤。物理地址过滤属于硬件认证,而不是用户认证。这种方式要求 AP 中的 MAC 地址列表必须随时更新。如果用户增加,则扩展能力变差,效率会随着终端数目的增加而降低,因此只适用于小型网络规模。

非法用户通过网络监听就可获得合法的 MAC 地址表，而 MAC 地址并不难修改，因而非法用户完全可以通过盗用合法用户的 MAC 地址非法接入。MAC 地址过滤如图 9-1 所示。

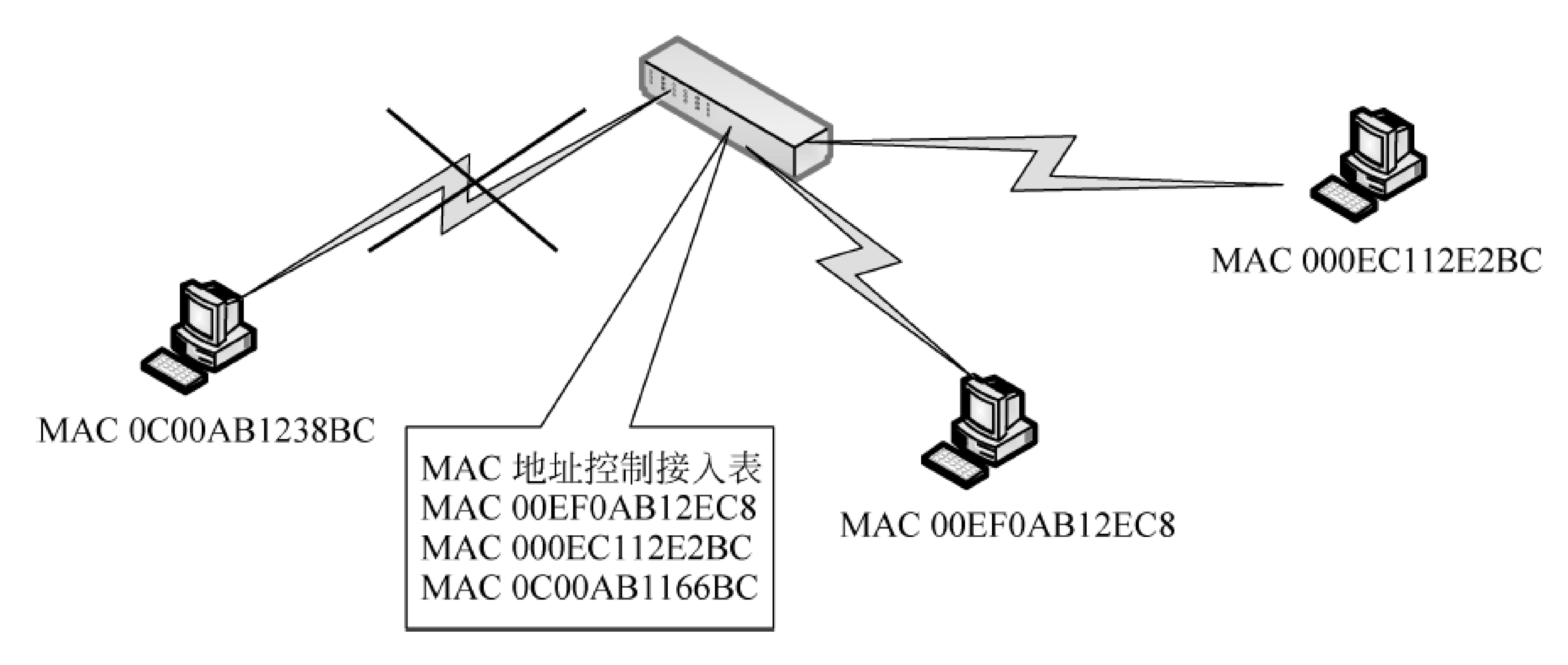


图 9-1　MAC 地址过滤

9.3.2　服务区标识符匹配

无线客户端必须设置与无线访问点 AP 相同的 SSID 才能访问 IP。利用 SSID 设置，可以很好地进行用户群体分组，避免任意漫游带来的安全和访问性能降低的问题。可以通过设置隐藏接入点及 SSID 区域的划分和权限控制来达到保密的目的，因此可以认为 SSID 是一个简单的口令，通过提供口令认证机制，确保一定程度的安全。服务区标识符匹配如图 9-2 所示。

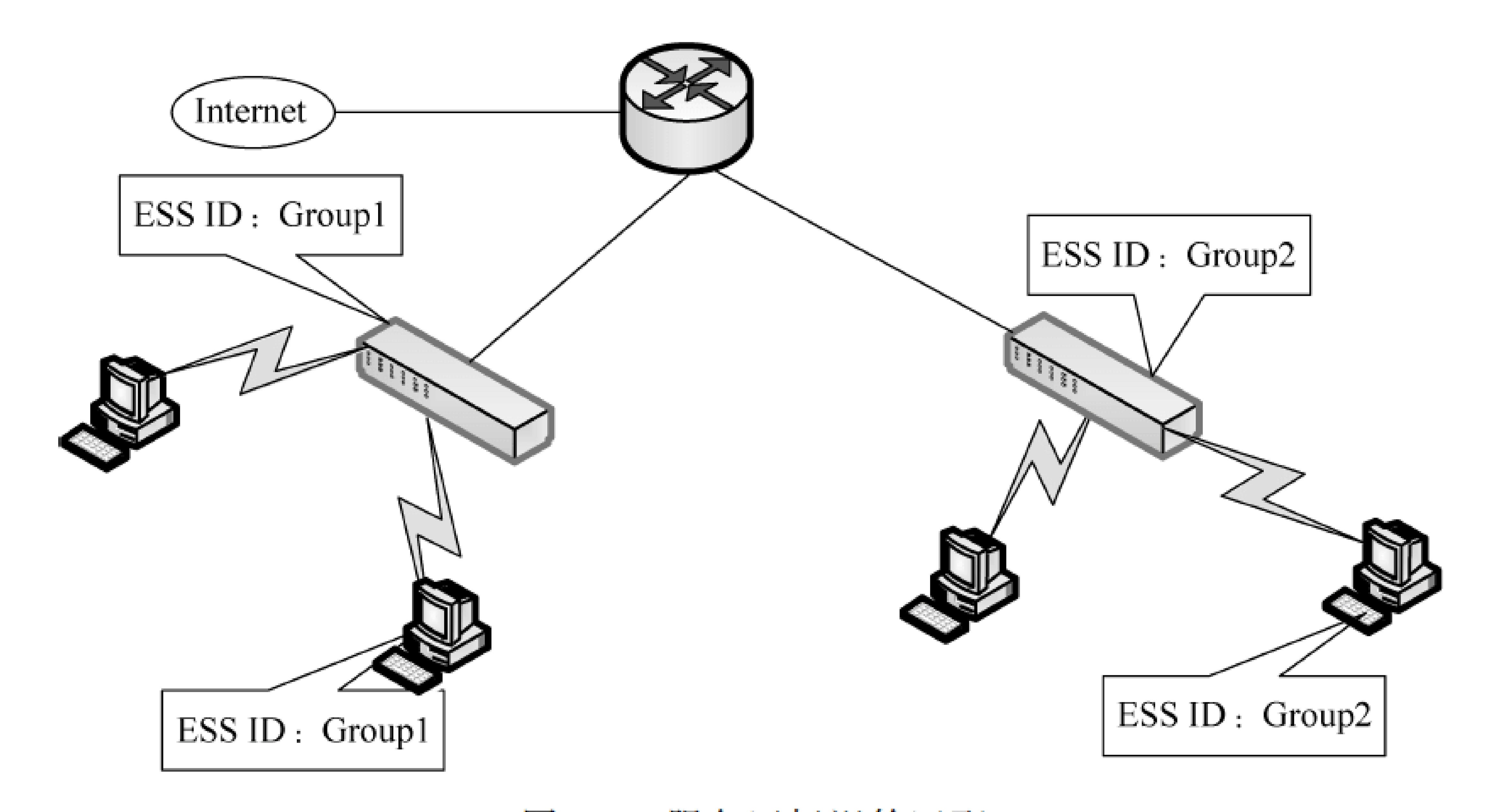


图 9-2　服务区标识符匹配

如果配置 AP 向外广播其 SSID，那么安全程度将下降，因为一般情况下用户自己配置客户端系统，很多人都知道该 SSID，所以很容易共享给非法用户。有的厂家支持所有 SSID 方式，只要无线工作站在某个 AP 范围内，客户端都会自动连接到 AP，这将跳过 SSID 安全功能。

9.3.3 连线对等保密

IEEE 802.11b 标准定义了一个加密协议 WEP(Wired Equivalent Privacy),用来对无线局域网中的数据流提供安全保护。该协议采用 RC4 流加密算法,提供的功能主要包括以下两点。

(1) 访问控制:防止没有 WEP 密钥的非法用户访问网络。

(2) 保护隐私:通过加密手段保护无线局域网上传输的数据。

1. WEP 加密过程

WEP 加密过程如图 9-3 所示。从图中可以看出,在对明文数据的处理上采用了两种运算:一是对明文进行的流加密运算(即异或运算);二是为了防止数据被非法篡改而进行的数据完整性检查向量(ICV)运算。

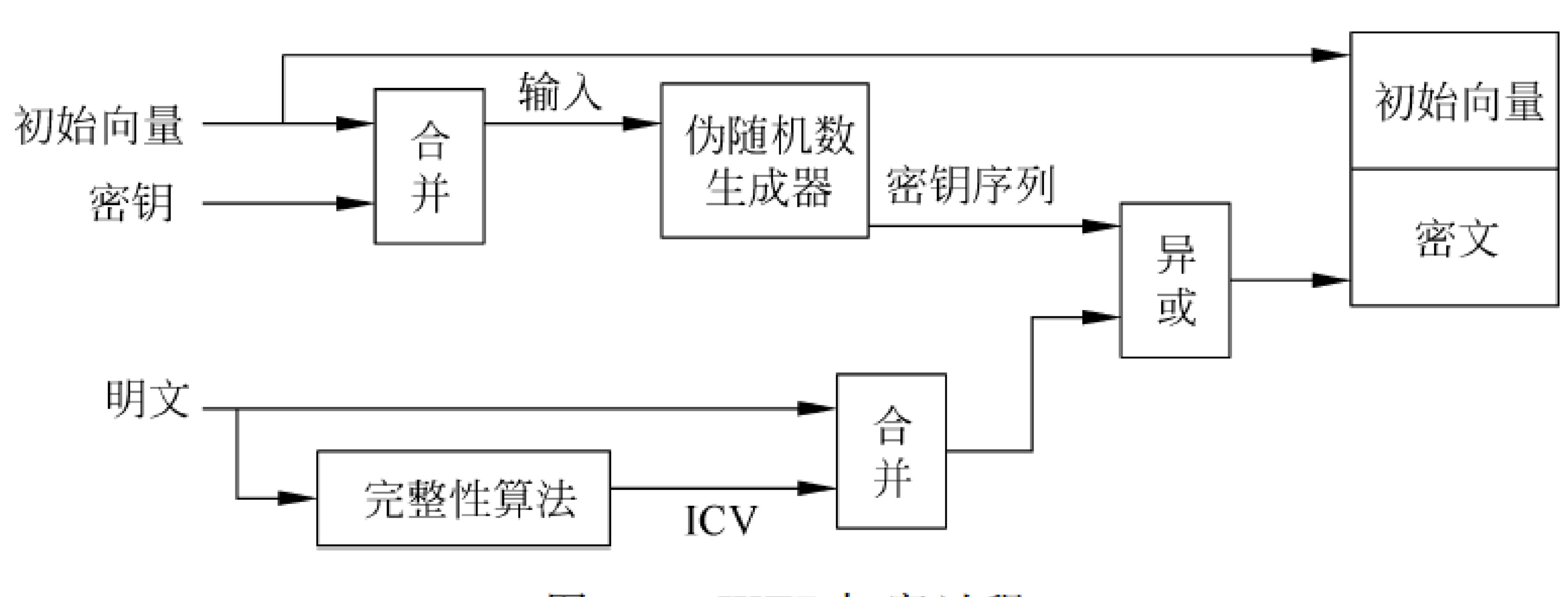


图 9-3 WEP 加密过程

(1) 40 位的加密密钥与 24 位的初始向量(IV)结合在一起,形成 64 位长度的密钥。

(2) 生成的 64 位密钥被输入到伪随机数生成器(PRNG)中。

(3) 伪随机数生成器输出一个伪随机密钥序列。

(4) 生成的序列与数据进行位异或运算,形成密文。

为了保证数据不被非法篡改,一种完整性算法(CRC32)会应用在明文上,生成 32 位的 ICV。明文与 32 位的 ICV 合并后被加密,密文与 IV 一起被传输到目的地。

2. WEP 解密过程

WEP 解密过程如图 9-4 所示,为了对数据流进行解密,WEP 进行如下操作。

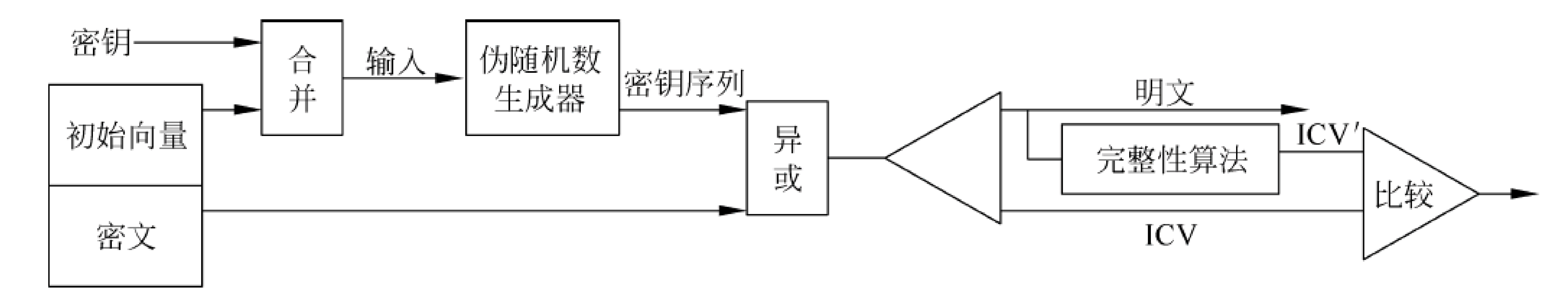


图 9-4 WEP 解密过程

(1) 接收到的 IV 被用来产生密钥序列。

(2) 加密数据与密钥序列一道产生解密数据和 ICV。

(3) 解密数据通过数据完整性算法生成 ICV。

(4) 将生成的 ICV 与接收到的 ICV′进行比较。如果不一致，将错误信息报告给发送方。

3. WEP 认证方法

一个客户端如果没有被认证，将无法接入无线局域网，因此必须在客户端设置认证方式，而且该方式应与接入点采用的方式兼容。IEEE 802.11b 标准定义了两种认证方式：开放系统认证和共享密钥认证。

1) 开放系统认证

开放系统认证是 IEEE 802.11 协议采用的默认认证方式。开放系统认证对请求认证的任何人提供认证。整个认证过程通过明文传输完成，即使某个客户端无法提供正确的 WEP 密钥，也能与接入点建立联系。

2) 共享密钥认证

共享密钥认证采用标准的挑战/响应机制，以共享密钥来对客户端进行认证。该认证方式允许移动客户端使用一个共享密钥来加密数据。WEP 允许管理员定义共享密钥，没有共享密钥的用户将被拒绝访问。用于加密和解密的密钥也被用于提供认证服务，但这会带来安全隐患。与开放系统认证相比，共享密钥认证方式能够提供更好的认证服务。如果一个客户端采用这种认证方式，它必须支持 WEP。WEP 认证过程如图 9-5 所示。

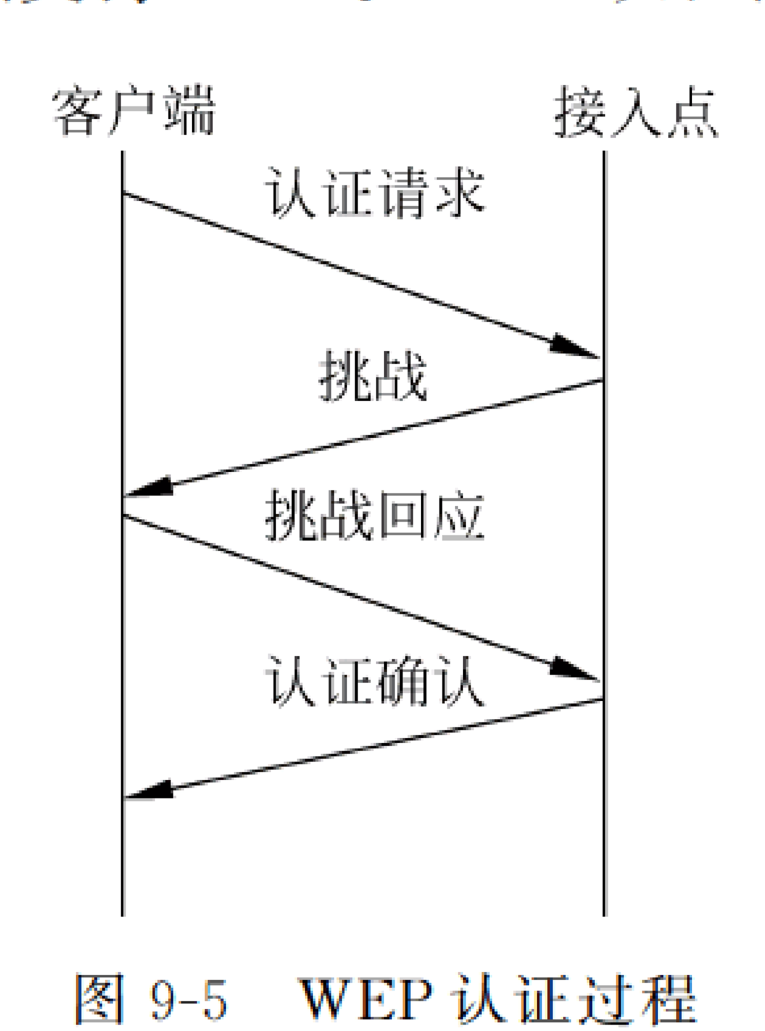


图 9-5　WEP 认证过程

4. WEP 密钥管理

共享密钥被存储在每个设备的管理信息数据库中。虽然 IEEE 802.11 标准没有指出如何将密钥分发到各个设备上，但它提到了以下两种解决方案。

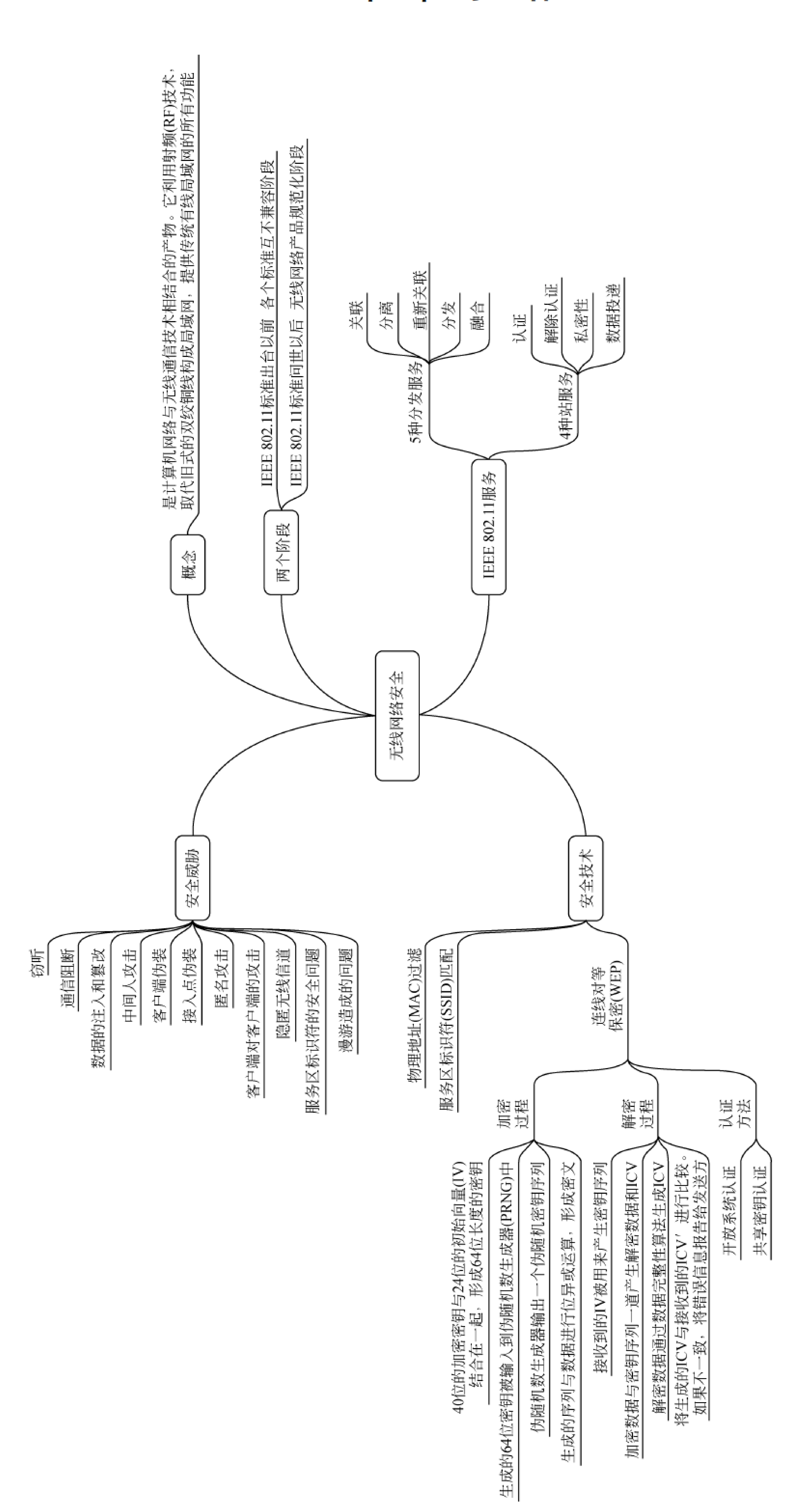
(1) 各设备与接入点共享一组共 4 个默认密钥。

(2) 每个设备与其他设备建立密钥对关系。

第一种方案提供了 4 个密钥。如果一个客户端获得了这些默认密钥，该客户端就可以与整个子系统的所有设备进行通信。客户端或接入点可以采用这 4 个密钥中的任意一个来实施加密和解密运算。这种方案的缺点是，如果默认密钥被广泛分发，它们就可能被泄漏。

第二种方案中，每个客户端都要与其他所有设备建立一个密钥对映射表，每个不同的 MAC 地址都有一个不同的密钥，且知道此密钥的设备较少，所以这种方案更安全。虽然这种方案减小了受攻击的可能性，但是随着设备数量的增加，密钥的人工分发会变得很困难。

9.4 本章小结


无线网络安全
概念
是计算机网络与无线通信技术相结合的产物。它利用射频(RF)技术，取代旧式的双绞铜线构成局域网，提供传统有线局域网的所有功能
两个阶段
IEEE 802.11标准出台以前 各个标准互不兼容阶段
IEEE 802.11标准问世以后 无线网络产品规范化阶段
IEEE 802.11服务
5种分发服务
关联
分离
重新关联
分发
融合
4种站服务
认证
解除认证
私密性
数据投递
安全威胁
窃听
通信阻断
数据的注入和篡改
中间人攻击
客户端伪装
接入点伪装
匿名攻击
客户端对客户端的攻击
隐匿无线信道
服务区标识符的安全问题
漫游造成的问题
安全技术
物理地址(MAC)过滤
服务区标识符(SSID)匹配
连线对等保密(WEP)
加密过程
40位的加密密钥与24位的初始向量(IV)结合在一起，形成64位长度的密钥
生成的64位密钥被输入到伪随机数生成器(PRNG)中
伪随机数生成器输出一个伪随机密钥序列
生成的序列与数据进行位异或运算，形成密文
解密过程
接收到的IV被用来产生密钥序列
加密数据与密钥序列一道产生解密数据和ICV
解密数据通过数据完整性算法生成ICV
将生成的ICV与接收到的ICV'进行比较。如果不一致，将错误信息报告给发送方
认证方法
开放系统认证
共享密钥认证

9.5 习　　题

一、填空题

1. 无线局域网是利用(　　)技术，取代旧式的双绞铜线构成局域网。

2. 没有基站的无线局域网又叫作(　　)。

3. IEEE 802.11 定义了 5 种分发服务，分别是关联、分离、重新关联、分发、(　　)。

4. WEP 加密过程中，对明文数据的处理采用两种运算，一是对明文进行的(　　)运算，二是数据完整性检查向量运算。

5. IEEE 802.11b 标准定义了两种认证方式，分别是开放系统认证和(　　)认证。

二、选择题

1. 以下(　　)是无线局域网最大的问题。

A. 可靠性低　　B. 安全性差
C. 传输速率低　　D. 移动通信能力弱

2. 关于 WEP，以下描述错误的是(　　)。

A. 一次性密钥不会重复
B. 用循环冗余码检测数据完整性
C. 伪随机数生成算法作为产生一次性密钥的单向函数
D. 采用流密码体制

3. 关于 WEP 加密，以下描述错误的是(　　)。

A. 终端和 AP 必须具有相同的密钥 K
B. 为了同步一次性密钥，发送端需要向接收端发送 IV 明文
C. 黑客无法通过嗅探经过无线网络传输的信息获得密钥 K
D. 黑客无法破译嗅探到的经过无线网络传输的密文

4. 关于 WEP 加密，以下描述错误的是(　　)。

A. 共享密钥是授权接入 BSS 的授权标识符
B. 共享密钥长度可以是 40 位或者 104 位
C. 一次性密钥的数量与共享密钥长度无关
D. 一次性密钥的长度等于共享密钥的长度

5. 关于 WEP 鉴别机制，以下描述错误的是(　　)。

A. 共享密钥是授权终端接入的授权标识符
B. AP 通过判断终端能否计算出特定 IV 下的一次性密钥判断终端是否拥有共享密钥
C. 通过嗅探可以获取特定 IV 下的一次性密钥
D. 通过嗅探可以获取共享密钥

三、判断题

1. IEEE 802.11 标准规定无线局域网的最小构件是基本服务集 BSS。

2. ZigBee 技术主要特点是通信距离短，成本低，但功耗大。

3. 服务区标识符(SSID)是无线接入点用于标识本地无线子网的标识符，如果用户不知道 SSID，接入点会拒绝该用户对本地子网的访问。

4. 物理地址过滤技术适用于大型网络。

5. 无线传感器网络是由大量传感器节点通过无线通信技术构成的自组网络。

四、综合题

1. 假定存在以下伪 WEP 协议，共享密钥为 4 位，取值 1010。IV 为 2 位，对应 2 位的 IV 的 4 种组合的 4 个一次性密钥如下。

101000：0010101101010101001011010100100…

101001：1010011011001010110100100101101…

101010：0001101000111100010100101001111…

101011：1111101010000000101010100010111…

假设所有消息的长度固定为 8 位，ICV 为 4 位，ICV 是消息的前 4 位与后 4 位异或运算结果。伪 WEP 分组包含 3 个字段：IV 字段、消息字段和 ICV 字段，对消息字段和 ICV 字段进行加密。

(1) 如果伪 WEP 协议在 IV＝11 的条件下发送消息 m＝10100000，求出 WEP 分组三个字段的值。

(2) 给出接收端解密该 WEP 分组、完成消息完整性检测的过程。

(3) 如果黑客截获了一个 WEP 分组(IV 值任意)，并在向接收端转发该 WEP 分组前篡改该 WEP 分组，由于黑客不知道共享密钥，因此没有任何 IV 值对应的一次性密钥。假定黑客翻转了 ICV 的每一位，则黑客还须翻转哪些其他位，才能使接收端成功完成完整性检测过程。

2. 假定 MAC 帧长度为 200B，无线局域网传输速率为 56Mb/s，求出发送完对应 IV 所有可能组合的 MAC 帧所需的时间(忽略 MAC 帧帧间间隔时间)。

第 10 章　网络安全方案设计

【本章学习目标】

- 理解网络安全方案的基本概念
- 重点掌握如何根据需求写出一份完整的网络安全的解决方案

10.1　网络安全方案概述

网络安全方案可以认为是一张施工的图纸,图纸的好坏直接影响到工程质量的高低。总的来说,网络安全方案涉及的内容比较多、比较广、比较专业和实际。

10.1.1　评价网络安全方案的质量标准

一份网络安全方案需要从以下 8 个方面来把握。

(1) 体现唯一性,由于安全的复杂性和特殊性,唯一性是评估安全方案最重要的一个标准。实际工作中,每一个特定网络都是唯一的,需要根据实际情况来处理。

(2) 对安全技术和安全风险有一个综合把握和理解,包括现在和将来可能出现的所有情况。

(3) 对用户的网络系统可能遇到的安全风险和安全威胁,结合现有的安全技术和安全风险,要有一个适合、中肯的评估,不能夸大,也不能缩小。

(4) 对症下药,用相应的安全产品、安全技术和管理手段,降低用户的网络系统在当前可能遇到的风险和威胁,消除风险和威胁的根源,增强整个网络系统抵抗风险和威胁的能力,增强系统本身的免疫力。

(5) 方案中要体现出对用户的服务支持。这是很重要的一部分,因为产品和技术,都将会体现在服务中,用服务来保证质量、提高质量。

(6) 在设计方案的时候,要明白网络系统安全是一个动态的、整体的、专业的工程,不能一步到位解决用户所有的问题。

(7) 方案出来后,要不断地和用户进行沟通,及时得到他们对网络系统在安全方面的要求、期望和所遇到的问题。

(8) 方案中所涉及的产品和技术,都要经得起验证、推敲和实施,要有理论根据,也要有实际基础。

将上面八点融会贯通,经过不断地积累经验,就能写出一份很实用的安全项目方案。

10.1.2 网络安全方案的框架

总体来说，一份安全解决方案的框架涉及 6 大方面，可以根据用户的实际需求取舍其中的某些方面。

1. 概要安全风险分析

对当前的安全风险和安全威胁做一个概括和分析，最好能够突出用户所在的行业，并结合其业务特点、网络环境和应用系统等。同时，要有针对性，如政府行业、电力行业、金融行业等，要体现很强的行业特点，使人信服和接受。

2. 实际安全风险分析

实际安全风险分析一般从以下 4 个方面进行分析。

(1) 确定要保护的资产及价值。如果不知道要保护什么内容，或者不知道要保护内容的情况，那就谈不上安全了。明确要保护的资产、资产的位置及资产的重要性是安全风险分析的关键。

(2) 分析信息资产之间的相互依赖性。由于某项资产的损失可能会导致其他资产的失效，因此，在确定资产的时候还要考虑资产之间的关联性。

(3) 确定存在的风险和威胁。确定了要保护的资产后，就应该分析对资产的潜在威胁以及受此威胁的可能性。威胁可以是任何可能对资产造成损失的个人、对象或事件，威胁也可能是故意的或偶然的。明确存在哪些弱点漏洞及这些弱点漏洞的风险级别，分析资产所面临的威胁、发生的可能性，以及一旦出现安全问题可能造成什么样的影响等。

(4) 分析可能的入侵者。要分析可能的入侵者存在的数量，进行攻击的可能性，进行攻击时威胁有多大等。

3. 网络系统的安全原则

安全原则体现在 5 个方面：动态性、唯一性、整体性、专业性和严密性。

(1) 动态性：不要把安全静态化，动态性是安全的一个重要的原则。网络、系统和应用会不断出现新的风险和威胁，这决定了安全动态性的重要性。

(2) 唯一性：安全的动态性决定了安全的唯一性，针对每个网络系统安全的解决，都应该是独一无二的。

(3) 整体性：对于网络系统所遇到的风险和威胁，要从整体来分析和把握，不能哪里有问题就补哪里，要做到全面地保护和评估。

(4) 专业性：对于用户的网络、系统和应用，要从专业的角度来分析和把握，不能是一种大概的做法。

(5) 严密性：整个解决方案要有一种很强的严密性，不要给人一种虚假的感觉，在设计方案时，需要从多方面对方案进行论证。

4. 安全产品

常用的安全产品有 5 种：防火墙、防病毒、身份认证、传输加密和入侵检测。结合用户的网络、系统和应用的实际情况，对安全产品和安全技术做比较和分析，分析要客观、结果要中肯，帮助用户选择最能解决他们所遇到问题的产品，不要求新、求好和求大。

(1) 防火墙：对包过滤技术、代理技术和状态检测技术的防火墙，都做一个概括和比较，结合用户网络系统的特点，帮助用户选择一种安全的产品，对于选择的产品，一定要从中立的角度来说明。

(2) 防病毒：针对用户的系统和应用的特点，对桌面防病毒、服务器防病毒和网络防病毒做一个概括和比较，详细指出用户必须如何做，否则就会带来什么的安全威胁，一定要中肯、适合，不要夸大和缩小。

(3) 身份认证：从用户的系统和用户的认证的情况进行详细的分析，指出网络和应用本身的认证方法会出现哪些风险，结合相关的产品和技术，通过部署这些产品和采用相关的安全技术，能够帮助用户解决系统和应用的传统认证方式所带来的风险和威胁。

(4) 传输加密：要用加密技术来分析，指出明文传输的巨大危害，通过结合相关的加密产品和技术，能够指出用户目前的情况存在哪些危害和风险。

(5) 入侵检测：对入侵检测技术进行详细的解释，在用户的网络和系统部署了相关的产品之后，详细分析现有的安全情况产生的影响。结合相关的产品和技术，指出用户的系统和网络会带来哪些好处，为什么必须要这样做，以及不这样做会带来什么后果。

5. 风险评估

风险评估是网络安全防御中的一项重要技术，也是信息安全工程学的重要组成部分。其原理是对采用的安全策略和规章制度进行评审，发现不合理的地方，采用模拟攻击的形式对目标可能存在的已知安全漏洞进行逐项检查，确定存在的安全隐患和风险级别。

6. 安全服务

安全服务不是产品化的东西，而是通过技术向用户提供的持久支持。对于不断更新的安全技术、安全风险和安全威胁，安全服务的作用变得越来越重要。

(1) 网络拓扑安全：结合网络的风险和威胁，详细分析用户的网络拓扑结构，根据其特点，指出现在或将来会存在哪些安全风险和威胁，并运用相关的产品和技术，来帮助用户消除产生风险和威胁的根源。

(2) 系统安全加固：通过风险评估和人工分析，找出用户的相关系统已经存在或是将来会存在的风险和威胁，并运用相关的产品和技术，来加固用户的系统安全。

(3) 应用安全：结合用户的相关应用程序和后台支撑系统，通过相应的风险评估和人工分析，找出用户和相关应用已存在或是将来会存在的风险，并运用相关的产品和技术，来加固用户的应用安全。

(4) 灾难恢复：结合用户的网络、系统和应用，通过详细的分析、针对可能遇到的灾难，制定出一份详细的恢复方案，把由于其他突发情况所带来的风险降到最低，并有一个良好的应付方案。

(5) 安全规范：制定出一套完善的安全方案，比如 IP 地址绑定、离开计算机时需要锁定等。结合实际分成多套方案，如系统管理员安全规范、网络管理员安全规范、高层领导的安全规范、普通员工的管理规范、设备使用规范和安全环境规范。

(6) 服务体系和培训体系：提供售前和售后服务，并提供安全产品和技术的相关培训。

10.2 网络安全案例需求

网络安全的唯一性和动态性决定了不同的网络需要有不同的解决方案。下面通过一个实际案例,学习如何提高安全方案设计能力。

项目名称:常盛信息集团公司(公司名为虚构)网络安全方案。

1. 案例背景

(1) 为了保证网络出口稳定可靠,企业向 ISP 申请了两条因特网线路,需要这两条线路做负载均衡和冗余备份。

(2) 管理性:网络设备需能够支持灵活多样的管理方式,可以减轻管理、维护的难度。

2. 项目要求

公司在网络安全方面提出了 5 方面的要求。

1) 安全性

全面有效地保护企业网络系统的安全,保护计算机硬件、软件、数据、网络不因偶然的或恶意破坏的原因遭到更改、泄漏和丢失,确保数据的完整性。

2) 可控性和可管理性

可自动和手动分析网络安全状况,适时检测并及时发现记录潜在的安全威胁,制定安全策略,及时报警、阻断不良攻击行为,具有很强的可控性和可管理性。

3) 系统的可用性

在某部分系统出现问题时,不影响企业信息系统的正常运行,具有很强的可用性和及时恢复性。

4) 可持续发展

满足常盛信息集团公司业务需求和企业可持续发展的要求,具有很强的可扩展性和柔韧性。

5) 合法性

所采用的安全设备和技术具有我国安全产品管理部门的合法认证。

3. 工作任务

该项目的工作任务包含 4 个方面。

(1) 研究常盛信息集团公司计算机网络系统的运行情况,对网络面临的威胁及可能承担的风险进行定性与定量的分析和评估。

(2) 研究常盛信息集团公司的计算机操作系统的运行情况,在操作系统最新发展趋势的基础上,对操作系统本身的缺陷及可能承担的风险进行定性和定量的分析和评估。

(3) 研究常盛信息集团公司的计算机应用系统的运行情况,在满足各级管理人员、业务操作人员的业务需求的基础上,对应用系统存在的问题、面临的威胁及可能承担的风险进行定性和定量的分析和评估。

(4) 根据以上的定性和定量的评估,结合用户需求和国内外网络安全最新发展趋势,有

针对性地制定常盛信息集团公司计算机网络系统的安全策略和解决方案，确保该公司计算机网络信息系统安全可靠地运行。

4. 案例拓扑结构

常盛信息集团公司网络安全方案拓扑结构如图10-1所示。

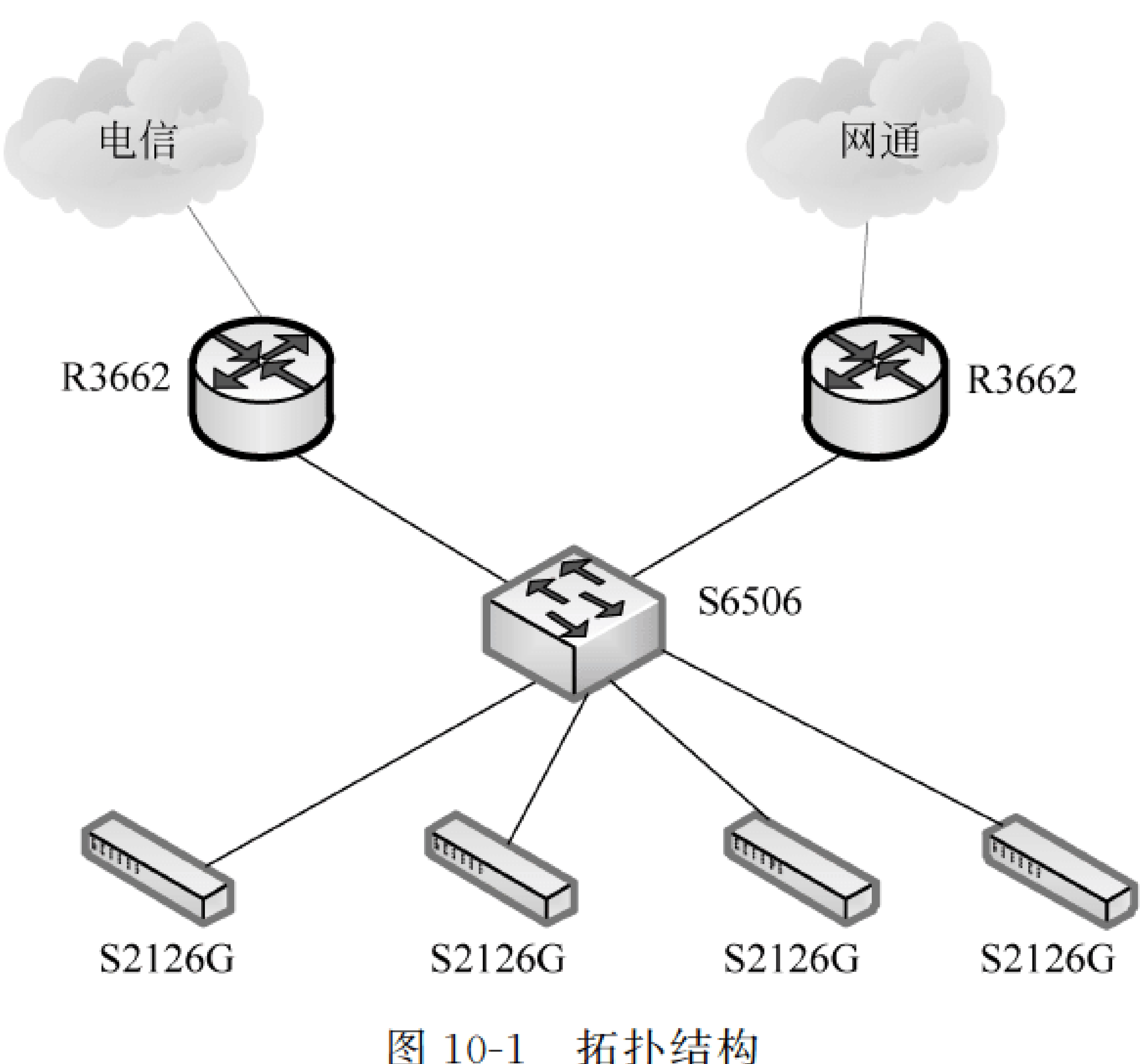


图10-1 拓扑结构

5. 地址规划

地址规则见表10-1所示。

表10-1 地址规划表

设　　备	IP地址	备　　注
R2624-A	192.168.1.253/24	R2624-A E0
R2624-B	192.168.1.254/24	R2624-B E0
虚拟备份组10	192.168.1.1/24	虚拟备份组10
虚拟备份组20	192.168.1.2/24	虚拟备份组20

10.3 网络安全方案设计

安卓网络安全公司(公司名为虚构)通过招标，以150万的工程造价得到了该项目的实施权。在解决方案设计中需要包含九方面的内容：公司背景简介、常盛信息集团的安全风险分析、完整网络安全实施方案的设计、实施方案计划、技术支持和服务承诺、产品报价、产品介绍、第三方检测报告和安全技术培训。

1. 公司背景简介

介绍安卓网络安全公司的背景需要包括：公司简介、公司人员结构、曾经成功的案例、产品或者服务的许可证或认证。

1）安卓网络安全公司简介

使用户对公司有一个好的印象，可以使工作更顺利地得以执行和完成，在这里不仅要介绍公司的背景，还要体现出公司的优越性、实力及公司的先进性。

2）公司的人员结构

公司的人员结构是用户了解公司实力的一个最直接途径，是一份必不可少的材料。

3）成功的案例

这里主要介绍公司以往的成功案例，特别是要指出与用户项目相似的成功案例，这样可以使用户相信公司有足够的经验来做好这件事情。

4）产品的许可证或服务的认证

产品的许可证是一份必不可缺的材料，因为只有取得许可证的安全产品，才允许在国内销售。网络安全属于提供服务的公司，只有通过国际认证才能取得用户更大的信任。

5）常盛信息集团公司实施网络安全意义

项目完成后，常盛信息集团公司的系统信息安全能到一个怎样的保护水平，要特别结合当前的安全风险和威胁来分析。

2. 安全风险分析

安全风险分析主要是对网络物理结构、网络系统和应用进行风险分析。

1）现有网络物理结构安全分析

详细分析常盛信息集团公司与各分公司的网络结构，包括内部网、外部网和远程网。

2）网络系统安全分析

详细分析常盛信息集团公司与各分公司网络的实际连接、因特网的访问情况、桌面系统的使用情况和主机系统的使用情况，找出可能存在的安全风险。

3）网络应用的安全分析

详细分析常盛信息集团公司与各分公司的所有服务系统以及应用系统，找出可能存在的安全风险。

3. 解决方案

解决方案包括 5 个方面。

1）建立常盛信息集团公司系统信息安全体系结构框架

通过具体分析常盛信息集团公司的具体业务和网络、系统、应用等实际应用情况，初步建立一个整体的安全体系结构框架。

2）技术实施策略

技术实施策略需要从网络结构安全、主机安全加固、防病毒、访问控制、传输加密、身份认证、入侵检测技术及风险评估等 8 个方面进行阐述。

3）安全管理工具

对安全项目中所用到的安全产品进行集中、统一、安全的管理和培训。

4）紧急响应

制定详细的紧急响应计划，及时响应用户的网络、系统和应用可能会遭到的破坏。

5）灾难恢复

制定详细的灾难恢复计划，及时把用户遇到的网络、系统和应用的破坏恢复到正常状态，并且能够消除产生风险和威胁的根源。

4. 实施方案

实施方案包括项目管理以及项目质量保证。

1）项目管理

(1) 项目流程：详细写出项目的实施流程，以保证项目的顺利实施。

(2) 项目管理制度：写出项目的管理制度，主要是保证项目实施的质量，项目管理主要包括人的管理、产品的管理和技术的管理。

(3) 项目进度：项目实施的进度表作为项目实施的时间标准，要全面考虑完成项目所需要的物质条件，计划出一个比较合适的时间进度表。

2）项目质量保证

(1) 执行人员的质量职责：规定项目实施相关人员的职责，如项目经理、技术负责人、技术工程师、后勤人员等，以保证整个安全项目的顺利实施。

(2) 项目质量的保证措施：严格制定出保证项目质量的措施，主要的内容涉及参与项目的相关人员、项目中涉及的安全产品和技术、用户派出支持该项目的相关人员的管理。

(3) 项目验收：根据项目的具体情况，与用户确定项目验收的详细事项，包括安全产品、技术、完成情况、达到的安全目的等验收。

5. 技术支持和服务承诺

技术支持和服务承诺包括技术支持的内容和技术支持的方式。

1）技术支持的内容

技术支持的内容包括安全项目中所包括的产品和技术的服务，提供的技术和服务包括以下内容。

(1) 安装调试项目中所涉及的全部产品和技术。

(2) 安全产品以及技术文档。

(3) 提供安全产品和技术的最新信息。

(4) 服务期内免费产品升级。

2）技术支持方式

安全项目完成以后提供的技术支持服务，包括以下 4 点。

(1) 客户现场 24 小时支持服务。

(2) 客户支持中心热线电话。

(3) 客户支持中心 E-mail 服务。

(4) 客户支持中心 Web 服务。

6. 产品报价

项目所涉及全部产品和服务的报价。

7. 产品介绍

常盛信息集团公司安全项目中所有涉及的产品介绍，主要是使用户清楚所选择的产品

是什么，不用很详细，但要描述清楚。

8. 第三方检测报告

由一个第三方的中立机构，对实施好的网络安全构架进行安全扫描与安全检测，并提供相关的检测报告。

9. 安全技术培训

1）管理人员的安全培训

安全培训主要是针对公司非技术的管理人员的培训，提高他们对安全的重视程度。主要应对4个方面的内容进行培训。

（1）网络系统安全在企业信息系统中的重要性。

（2）安全技术能够带来的好处。

（3）安全管理能够带来的好处。

（4）安全集成和网络系统集成的区别。

2）安全技术基础培训

安全技术基础培训主要针对网络系统管理员、安全管理相关人员的技术培训，使他们能够增强安全意识，了解基本的安全技术，能够分辨出网络、系统和应用中可能存在的安全问题，并且能够采用相关的安全技术、产品或服务来防范。培训的内容包括7个方面。

（1）系统安全、网络安全和应用安全的概述。

（2）系统安全的风险、威胁和漏洞的详细分析。

（3）网络安全的风险、威胁和漏洞的详细分析。

（4）应用安全的风险、威胁和漏洞的详细分析。

（5）安全防范措施的技术和管理。

（6）安全产品功能的简单分类。

（7）黑客攻击技术。

3）安全攻防技术培训

对网络系统管理员进行黑客攻击的手段、原理和方法的培训，使他们能够掌握黑客攻击的技术，并能运用到实际的工作中，有能力来保护网络、系统和应用的安全。

4）Windows 系统、UNIX 系统安全管理培训

这是主要针对网络管理员和系统管理员的系统安全技术培训，详细介绍操作系统的安全风险、安全威胁和安全漏洞等，使网络管理员和系统管理员能够独立配置安全系统，独立维护操作系统的安全。

5）安全产品的培训

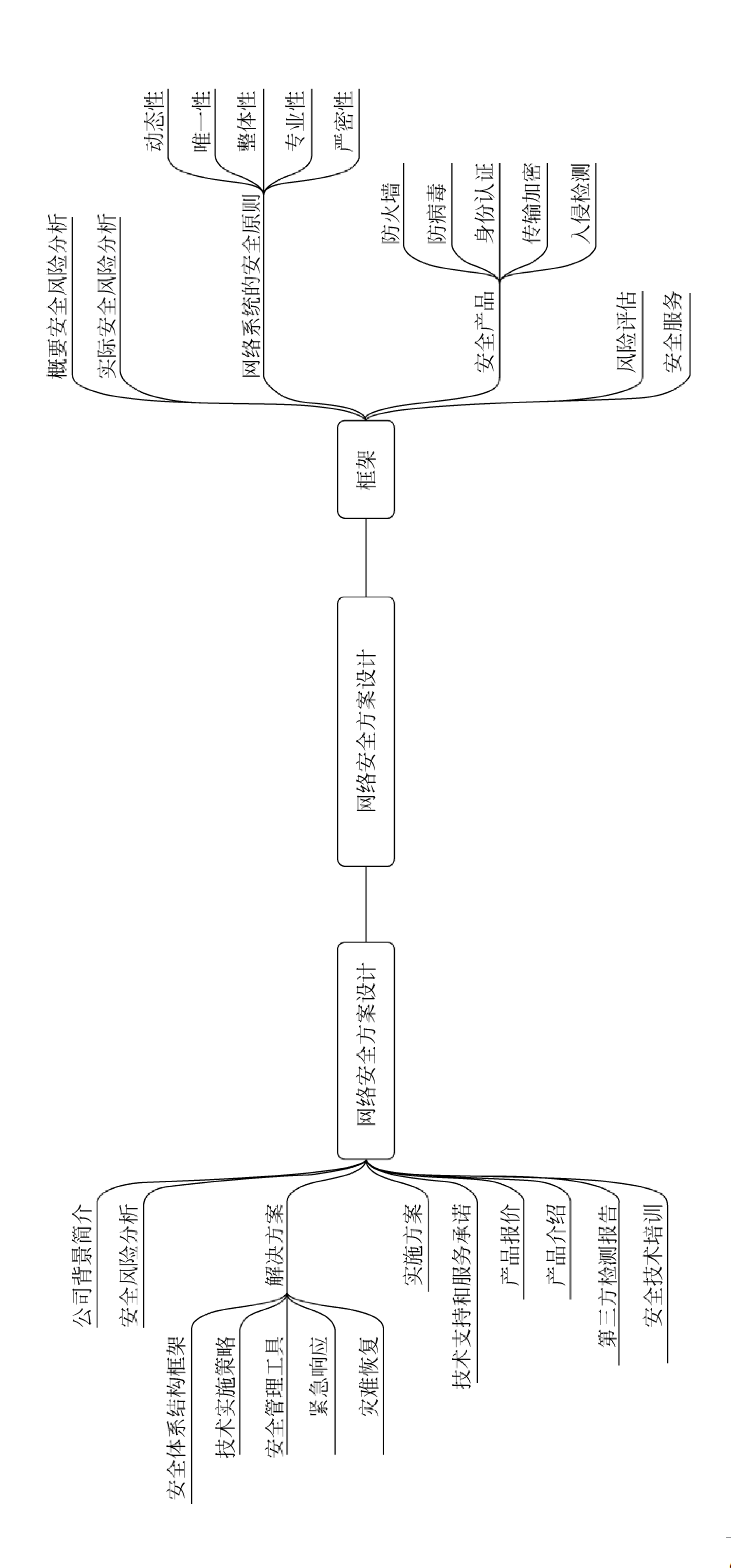
这是主要针对安全项目中所用到的安全产品向有关人员提供培训，培训的内容一般包括以下三个方面，可以根据实际情况进行删减。

（1）安全产品的原理，如防火墙技术、入侵检测技术等。

（2）各种安全产品在安全项目中的作用、重要性和局限性。

（3）安全产品的使用、维护和安全。

10.4 本章小结


网络安全方案设计
网络安全方案设计
框架
概要安全风险分析
实际安全风险分析
网络系统的安全原则
动态性
唯一性
整体性
专业性
严密性
安全产品
防火墙
防病毒
身份认证
传输加密
入侵检测
风险评估
安全服务
公司背景简介
安全风险分析
解决方案
安全体系结构框架
技术实施策略
安全管理工具
紧急响应
灾难恢复
实施方案
技术支持和服务承诺
产品报价
产品介绍
第三方检测报告
安全技术培训

10.5 习　　题

一、选择题

1. 一份好的计算机网络解决方案，不仅要考虑到技术，还要考虑到(　　)。

   A. 软件和硬件　　B. 机房和电源　　C. 策略和管理　　D. 加密和认证

2. 在进行计算机网络安全设计、规划时，不合理的是(　　)。

   A. 只考虑安全的原则　　B. 易操作性原则

   C. 适应性、灵活性原则　　D. 多重保护原则

3. 下列关于网络安全解决方案的描述，错误的是(　　)。

   A. 一份好的网络安全解决方案，不仅要考虑到技术，还要考虑策略和管理

   B. 一个网络的安全体系结构必须与网络的安全需求相一致

   C. 良好的系统管理有助于增强系统的安全性

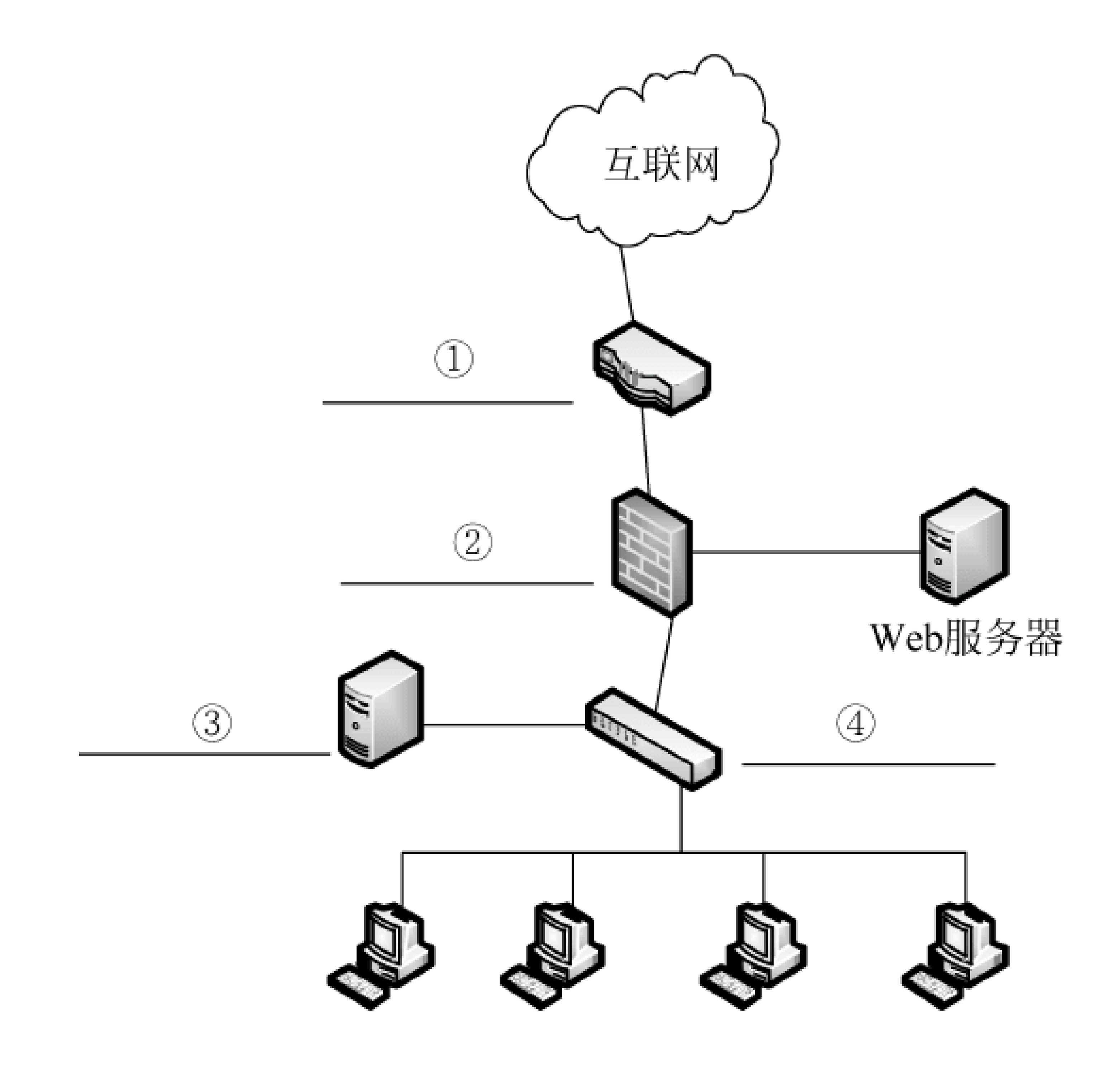
   D. 确保网络的绝对安全是制定一个网络安全解决方案的首要条件

二、综合题

某企业的网络安全设备配置拓扑如下图所示。

(1) 选用适当的网络安全设备填入图中①～④处，可选网络安全设备有：路由器、防火墙、中心交换机、身份认证服务器。

(2) 请为该企业设计网络安全解决方案。



图书资源支持

感谢您一直以来对清华版图书的支持和爱护。为了配合本书的使用，本书提供配套的资源，有需求的读者请扫描下方的“书圈”微信公众号二维码，在图书专区下载，也可以拨打电话或发送电子邮件咨询。

如果您在使用本书的过程中遇到了什么问题，或者有相关图书出版计划，也请您发邮件告诉我们，以便我们更好地为您服务。

我们的联系方式：

地　　址：北京市海淀区双清路学研大厦 A 座 701

邮　　编：100084

电　　话：010-83470236　010-83470237

资源下载：http://www.tup.com.cn

客服邮箱：2301891038@qq.com

QQ：2301891038（请写明您的单位和姓名）

资源下载、样书申请



书圈



扫一扫，获取最新目录



课　程　直　播

用微信扫一扫右边的二维码，即可关注清华大学出版社公众号“书圈”。